Allied Telesyn International

*Turbo*Stack™

AT-S10

*Management Software for Turbo*Stack *Hubs*

User's Guide

PN 613-10655-00 Rev. A

© Copyright 1997 Allied Telesyn International Corp.
All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn International Corp.

Allied Telesyn reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn has been advised of, known, or should have known, the possibility of such damages.

AT-View and CentreCOM are registered trademarks of Allied Telesyn International Corp.

*Turbo*Stack, Omega Local, and Omega Remote are trademarks of Allied Telesyn International Corp.

UNIX is a registered trademark of X/Open Company Limited. Windows is a trademark of Microsoft Corporation.

All company names, logos, and product designations that are trademarks or registered trademarks are the property of their owners.

Table of Contents

Preface vii
Audience vii
How this Guide is Organized vii
Document Conventions viii
Related Documentation ix

Chapter 1

Overview 1
Software Features 1
The TurboStack Hub Configurations 2
Planning to Manage the Hubs 3
Local management 3
Remote management 3
TCP/IP Networks 4
TCP/IP with BootP 4
TCP/IP without BootP 4
Non-TCP/IP Networks 4
Interoperability with AT-S4 4

Chapter 2

Getting Started 5
Connecting a Terminal 5
Starting a Session 6
Naming the hub 6
Entering an IP address 6
Assigning a Hub Name 7
Entering an IP Address 8
Working with the Omega Menus 10
Selecting Menu Options 10
Configuring Hub Modules in a Chassis 11
Ending a Session 12
Managing Remote Hubs 12
Using AT-View® 13

Chapter 3

Management Menus 15
Main Menu 15
Port Status Menu 17
Port Configuration Menu 18
Port Enable and Port Disable 18
Enable port with automatic partitioning 18
Disable port 18
Reconnection 19
Standard IEEE reconnection algorithm 19
Alternate reconnection algorithm 19
Link Test 19
Link Test On 19
Link Test Off 19
Polarity 19
Polarity Correction 19
No Polarity Correction 19
Change Port Name 19
Zero Counters 19
Redundant Links Configuration 20
Port Learning 25
AUI Port Configuration 25
Hub Statistics Menu 26
Hub Overview 27
Individual Port Overview 28
Zero Counters 28
Module Statistics Menu 29
Module Overview 29
Individual Port Overview 30
Zero Counters 30
Security/Source Address Table Menu 31
Source Address Table (SAT) 31
Learning Mode 33
Learning On 33
Security On 33
Administration Menu 35
Hub Name Menu 35
Module Name Menu 36
Omega Options 36
Password 36
Timeout 36
Omega Local 37
Omega Remote 37
Network Parameters Menu 37
Hub IP Address 38
Subnet Mask 38
Gateway Address 38
SNMP Manager Address 39
“Get” Community String 39
“Set” Community String 39
“Trap” Community String 40
Download Password 40
Location String 40
Contact String 41

Terminal Configuration Menu 41
ANSI or DEC VT-100 Terminal 42
Generic or "Dumb" Terminal 42
Data Rate 43
Language Menu 43
Update Selected Node 44
Update All Nodes 44
Reset to Defaults 45
Activity Monitor 45
EtherMeter 46
Diagnostics 46
Connect to a Remote Hub 47

Chapter 4

Fault Tolerance 49
Department Concentrator Reconfiguration 50
Module Failures 50
Configuration Data 51
Precedence 51
Voting 52
Swapping Modules to Retain Configuration Data 52

Chapter 5

Software Upgrades 53
Using the Firmware Cassette 54
Using the Download Menus 56
TFTP 58

Appendix A

Technical Support Fax Order 59
Incident Summary 59

Appendix B

AT-S10 Management Software User's Guide Feedback 61

Appendix C

Where To Find Us 63

Appendix D

Index 65

Preface

This guide describes the procedures to manage the *Turbo*Stack™ series of management hubs using the software, AT-S10, and its management agent, Omega.

The software is pre-installed in *Turbo*Stack management hubs.

Audience

This guide is written for you, the technical person responsible for managing *Turbo*Stack hubs. You must be familiar with Ethernet networks and the devices used in these networks.

Before using this guide, you must have at least one management *Turbo*Stack hub installed and operational in the network.

How this Guide is Organized

This guide consists of the following chapters and appendices:

Chapter 1, "Overview," describes the features of the pre-installed AT-S10 software and Omega, the management agent.

Chapter 2, "Getting Started," describes the initial setup steps for you to begin managing your *Turbo*Stack hub, and also introduces you to Omega's user interface.

Chapter 3, "Management Menus," describes the menus you use to configure and manage *Turbo*Stack hubs.

Chapter 4, "Fault Tolerance," describes the process by which modules in the chassis automatically adapt to module failures and preserve configuration data.

Chapter 5, “Software Upgrades,” describes the procedures to install the latest software in *Turbo*Stack hubs.

Appendix A, “Technical Support Fax Order,” is a form on which you record problems with the product to send to Allied Telesyn Technical Support.

Appendix B, “AT-S10 Management Software User’s Guide Feedback,” is a form on which you record your comments on this guide to send to Allied Telesyn Technical Communication.

Appendix C, “Where To Find Us,” provides information on Allied Telesyn’s worldwide locations.

Refer to Allied Telesyn’s web site for a glossary of networking terms. See Appendix C for the location.

Document Conventions

The following conventions are used in presenting information in this guide:

- This guide refers to two or more chassis-mounted hubs as a *department concentrator*. The term *hub* refers to either a standalone hub or a department concentrator configuration. Each installed hub in a chassis is called a *module*.
- Menus, commands, prompts, file and pathnames, and other system-related information displayed by the user interface appear in Courier typeface; for example:

 Select `Administration` from the main menu.
- Text in **boldface** are entries you must type; for example:

 Enter **N** to get the `Network Parameters` menu.
- When directed to enter something, you must type the required characters and then press the **Return** key. This guide will not direct you to press the **Return** key after making an entry unless the action will cause a change to take effect. For example:

 1. Enter **0** for no parity.
 2. Press **Return** twice to enable automatic baud detection.

 This means you press the **Return** key a total of three times: after entering the parity value in Step 1 and to let the hub software check for the terminal’s baud rate in Step 2.
- A procedure icon and heading usually denotes an action or a series of actions you must perform. For example:

 To connect to a remote hub:

 Numbered steps may follow.

- Note icon:

 NOTE

 Notes indicate additional information.

- Caution icon:

 CAUTION

 Cautions tell you that a specific action or an omission of a step will result in equipment damage or loss of data.

- Attention icon:

 ATTENTION

 Attentions tell you about specific actions that are important and their omission might lead to minor errors.

Related Documentation

The following Allied Telesyn publications provide information to supplement this guide:

TurboStack Ethernet Hubs with Management Installation Manual

TurboStack Ethernet Slave/Manageable Hubs Installation Manual

TurboStack 4-, 7-, and 8-Slot Chassis and Backplanes Installation Manual

TurboStack AT-TSAx Appliqués Installation Manual

Chapter 1
Overview

This chapter describes:

- The features of AT-S10 and the management agent Omega
- An overview of *Turbo*Stack hub configurations in relation to hub management
- Information on managing a *Turbo*Stack hub on your network
- The interoperability of the AT-S10 software with AT-S4

Software Features

Figure 1 shows the 12-port AT-TS12TR TurboStack hub.

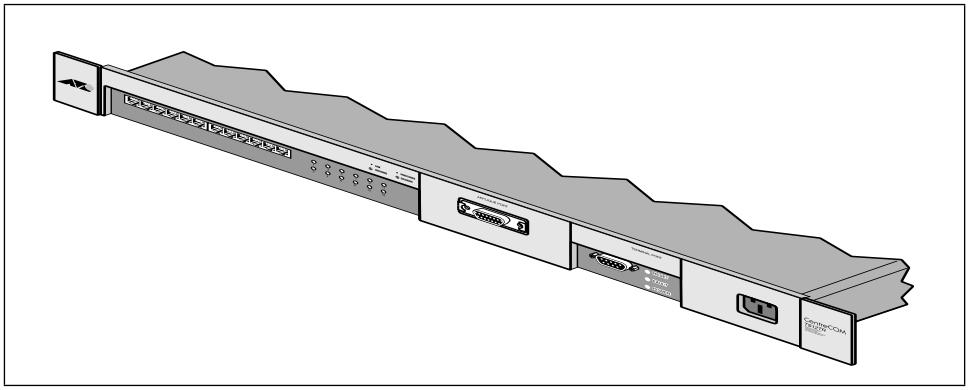


Figure 1: AT-TS12TR *Turbo*Stack Hub

Each manageable hub is factory-configured with the AT-S10 software and has the following software features:

- IEEE 802.3 compliance; Ethernet Version 1.0 and 2.0 compatible repeater functionality
- Two types of network management capability:
 - — SNMP
 - — **Omega** via ASYNC ASCII terminal port (Omega Local™) or Telnet (Omega Remote™)

- ❑ Software upgrade through firmware cassette or downloading via the network
- ❑ Redundant links help to ensure connectivity to a critical network resource, such as the corporate backbone or a server
- ❑ Inventory control through storage of multiple addresses on MAC address table
- ❑ Comprehensive security features to enable:
 - — Restricted access to the hub's management interface
 - — Restricted access to specific ports
 - — Manual updates to the MAC address table by the user when secure mode locks MAC address table (no learning)

The TurboStack Hub Configurations

Each manageable *Turbo*Stack hub is a single building block for both standalone (hub) and chassis (department concentrator) configurations. Allied Telesyn supplies the *Turbo*Stack chassis that offers two configurations to enable you to build and reconfigure your networks easily, efficiently, and at minimum expense:

- ❑ A standard configuration where a fully populated department concentrator behaves as a single hub in the network topology.
- ❑ A segmented configuration that holds up to six *Turbo*Stack hubs and either an AT-TS90TR or an AT-TS95TR switch occupying the bottom slot. Each hub is independently connected to the network backbone through the switch.

The management hub in the uppermost slot is the **master** module. It provides agent services for the entire concentrator. Should the master module fail, the **backup** takes over the master functions automatically (as long as the backup module is also a managed hub). You can hot swap any module to trace faults or reconfigure the concentrator without network downtime or interrupting hub management functions.

The *Turbo*Stack series also includes "slave" modules that are not manageable as standalone devices (the AT-TS12FS/XX, AT-TS24TS, and AT-TS24TRS models). The slave models, however, can be managed through a master module housed in the same department concentrator chassis. In such a department concentrator chassis, the configuration, status, and statistical information of slave hubs appear on the network management displays and can be manipulated in the same way as the data from the manageable modules.

NOTE

This manual refers to two or more chassis-mounted hubs as a *department concentrator*. The term *hub* refers to either a standalone hub or a department concentrator configuration. Each installed unit in a chassis is called a *module*.

For information on the hardware installation and connectivity aspects of manageable TurboStack hubs, see the separate *TurboStack Ethernet Hubs With Management Installation Manual* shipped with each hub.

Planning to Manage the Hubs

Before installing and connecting *Turbo*Stack hubs at various site locations (such as in closets in a single building, in closets on different floors, or in different buildings), decide on the number of hubs in your network and where each hub is to be located. Advanced planning facilitates the assignment of hub names and IP addresses if you use them. Planning also maximizes the efficiency of network management once your hubs are fully installed and operational.

If you have a limited number of workgroup PCs and devices located on the same floor, for example, you may decide to manage each hub locally in a standalone configuration.

If you have many geographically dispersed subnetworks, each connected to its own department concentrator, management of these multiple hubs remotely in a central-site configuration requires TCP/IP network management and a commercially available network management platform such as HP OpenView™.

Local management. If you want to manage the hub locally (Omega Local™), connect a terminal or a PC directly to its RS-232 port and access the Omega menus (see Chapter 3, "Terminal Configuration Menu," on page 41).

Remote management. From a hub you are managing locally, you can connect to remote *Turbo*Stack management hubs and manage them also.

You need one of the following:

- Its pre-configured MAC address, found on the edge of the right-hand plastic flap on t he front panel
- A unique IP address if you have TCP/IP (either you assign one to the hub or have your BootP server provide the parameters)
- A unique name that you assign via Omega

Detailed procedures are found in Chapter 2, "Getting Started."

NOTE

In a chassis configuration where all the manageable hubs share a common backplane, only the top (or master) module needs to have a TCP/IP address or hub name. For management purposes only, Omega views the modules in the chassis as a single hub within the network.

TCP/IP Networks

To manage the hub in TCP/IP, you first configure its IP parameters or at least assign a unique IP address to the hub. You have the option to manage using either SNMP or Omega Remote™ via Telnet.

TCP/IP with BootP. The function of the BootP utility within an IP server is to enter an IP address into the hub. Whenever you reset the hub or power it up, it transmits a request packet to the server every three seconds to obtain IP parameters.

If the requesting hub does not receive a BootP response after the third request, it continues to operate with a computed pseudo IP address based on its MAC address.

If the hub receives a BootP response, it extracts the IP address, Subnet Mask, or Gateway/Router address from the response packet and uses these parameters to configure itself until the next power-on or reset. Additionally, if the response packet specifies a filename and a TFTP host address, then the hub sends a TFTP `get` request to the specified host using the specified filename. This initiates a TFTP download of operating software and allows you to maintain downloaded server software.

NOTE

If only the master module loses power, the concentrator uses the IP address stored in the backup module. When the master module reinitializes, it does not send a BootP request packet because it obtains the configuration from the backup module.

TCP/IP without BootP. To manage the hub with SNMP or via Telnet, you must manually enter at least the IP address using the Omega menus. With or without BootP, entering a unique IP address via Omega ensures this parameter is always available.

Non-TCP/IP Networks

To manage the hub, connect a terminal to the hub (see Chapter 3, “Terminal Configuration Menu,” for the procedures). You may then start Omega and assign a unique name, or use the pre-configured MAC address.

Interoperability with AT-S4

AT-S4 is the management software for Allied Telesyn’s CentreCOM® hubs, the AT-3600 series. You can mix and match *Turbo*Stack and AT-3600 management hubs in a chassis; however, the advanced AT-S10 features will not be available. You need to insert an AT-S4 cassette version 3.0 or greater into the *Turbo*Stack hub to so it functions as an AT-3600. To return the *Turbo*Stack hub to its original software level, re-insert the AT-S10 cassette.

Proceed now to Chapter 2 to perform initial management setup.

Chapter 2

Getting Started

This chapter describes the following procedures:

- ❑ Connecting a terminal to the hub for local management
- ❑ Initial and optional configurations
- ❑ Starting an Omega session for initial setup
- ❑ Using the Omega menus
- ❑ Connecting to remote *Turbo*Stack hubs for remote management

Connecting a Terminal

Before proceeding, make sure you have installed the hub by following the procedures in the *TurboStack Ethernet Hubs with Management Installation Manual* and that the hub is functioning as a repeater.

Terminal connection for a local or standalone management involves the following preliminary set-up steps:

1. Connect the serial port of your terminal or PC to the RS-232 console port on the front of the hub. For a PC connection, use a straight-through 9-pin cable.
2. Turn on your terminal or PC and call up the terminal emulator program.
3. Check your screen display make sure the emulation options are set as follows:
 - ❑ Data bits: 8
 - ❑ Stop bits: 1
 - ❑ Parity: 0
 - ❑ Connector: Com1/Com2 (PC/terminal dependent)

 The Omega program supports automatic baud rate detection, so you do not have to configure baud rate on the terminal side.

NOTE

These configuration options apply whether you are using Windows or a DOS-based terminal emulator program. To be sure these options are always available, save them as an Omega file (i.e., **OMEGA.TRM**). If you have previously accessed Allied Telesyn devices with existing terminal settings, use the same ones without recreating a new **.TRM** file.

4. To activate the emulation program, press **Return** twice.

 This ensures configuration of the appropriate baud rate.

ATTENTION

Be sure you are using a full screen at your terminal or PC. Otherwise, you may not see all the characters and menu items displayed by the Omega agent.

You are done with terminal connection.

In future sessions using a PC running Windows, you only have to access Omega through the terminal emulator program. Pressing **Return** twice will display the main menu.

You are now ready to manage the hub as a standalone (or install it as a master module in a chassis) and perform initial configurations.

Starting a Session

Once you have established a connection to the hub from your terminal, the main menu of the Omega Local management program appears on your screen:

```
    Allied Telesyn International AT-TS24TR Stackable Hub: 4.0

Please select an option:

  Port status
  Hub Statistics
  Individual port overview
  Security/Source Address Table
  Administration
  Quit

->
```

Keep the menu displayed if you want to enter initial setups.

The procedures in this section are about configuring the following options:

Naming the hub. This is not required but will prove convenient when you start managing multiple hubs.

Entering an IP address. This is required if you have TCP/IP. If you are using a subnet mask and a router, you must enter their addresses also.

Assigning a Hub Name

While specifying an IP or MAC address is enough to communicate with the hub, names are more descriptive and easier to remember. For the same reason, plan to assign names to ports as well (described later in Chapter 3).

To name the hub:

1. Enter **A** for `Administration` from the main menu to get the `following screen`:

```
Please select an option:

Hub name
Module name
Omega Options

Network parameters
Terminal configuration

Language/langue/idioma/linguaggio/sprache

Send updated software to another hub
Update software in all hubs
Reset hub configuration to manufacturing defaults

Activity monitor
EtherMeter

Diagnostics

Connect to a remote hub

 ->
```

2. Enter **H** for `Hub name`.

 The following menu appears:

```
The Hub's current name is:
  Null (not currently configured)

Please enter a new name, or Return to retain the existing name:

 ->
```

3. Enter the hub name, for example, **Sunnyvale**.

 From now on, the name appears at the top of the menus.

You are done naming the hub. Through Omega, you can now connect to this hub by specifying its name.

CAUTION

Make sure each hub name is unique because the software does not validate duplicate hub names. If you use duplicate names, you might inadvertently connect, reconfigure, or download software to the wrong hub.

Entering an IP Address

This section applies only if you have TCP/IP.

The hub needs an IP address so you can communicate with it via Telnet or SNMP. Other parameters such as subnet mask and gateway addresses are also required if you have them. As discussed in Chapter 1, you may use BootP (if you have it) in your IP server to configure the hub with its IP parameters.

The following procedures ensure your hub is permanently configured with its own IP parameters, whether or not you have a BootP server.

To enter an IP address:

1. Enter **N** for `Network parameters` from the `Administration` menu.

 The following menu appears:

```
A: Ip address:                  Null (not configured)
B: Subnet mask:                 Null (not configured)
C: Gateway address:             Null (not configured)

D: SNMP Manager address:        Null (not configured)
E: SNMP Manager address:        Null (not configured)
F: SNMP Manager address:        Null (not configured)
G: SNMP Manager address:        Null (not configured)

H: Download Password:           *******

I: Get community string:        public
J: Set community string:        private
K: Trap community string:       public

L: Location:                    Null (not configured)
M: Contact:                     Null (not configured)
```

2. Enter **A** for `IP address` to get the following menu:

```
The current Hub IP Address is:
  Null (not currently configured)

Please enter a new value, or Return to retain the existing name:


Enter a value in the form of a.b.c.d, where a,b,c, and d are each in
the range 0-255. For example: 128.9.3.1

 ->
```

3. Enter the hub's IP address at the prompt.

 The `Network parameters` menu appears, displaying the IP address you entered.

NOTE

Each standalone hub in your TCP/IP network must have an IP address. However, in a concentrator configuration, only the master hub (the module in the uppermost slot) needs it. The network sees the concentrator as a single unit through the master.

4. Continue by entering the letter corresponding to the network parameter you want to configure, as follows:

 B: Subnet mask. This is required if you have it.

 C: Gateway address. This is required if you need to send packets from one IP network to another via a router.

 D through G: SNMP Manager address. You may enter the IP addresses of up to four network management servers that will receive SNMP trap messages. This parameter is optional.

 H: Download password. The default password is **ATS10**, shown in asterisks. The download process requires this password to send software from one hub to another, provided they are all *Turbo*Stack management hubs and they have the same download password. You may keep the default or change it. If you change the download password for this hub, it cannot accept software downloads from or download software to other switches that have a different password.

NOTE

The software automatically searches for this password during the download process without requiring you to enter it. This password is different from the optional system password you configure to limit access to the hub's management user interface.

 I through J: Community strings. The defaults for the `get`, `set`, and `trap` community strings are provided and you may keep them.

 K: Location. You may enter a 20-character text string to indicate the physical location of the hub, for example, **First Floor, Lab**, or any description that is useful to you. This parameter is optional and is used for SNMP management.

 L: Contact. You may enter a 20-character text string to indicate the name, phone number, or any useful information to help identify the person responsible for the hub. This parameter is optional and is used for SNMP management.

You just completed initial setup for local management of one hub. Other configuration options are available and the procedures are in Chapter 3. Most users keep the default, or customize selected options as required by their environment.

NOTE

If there are other standalone *Turbo*Stack hubs on the network and you are configuring their IP parameters for the first time, connect these hubs to the terminal and repeat the procedure.

To familiarize yourself with the Omega user interface, proceed to the next section.

Working with the Omega Menus

Once you are in session, the hub is locked from other session requests; for example, if using Omega Local, others cannot use Omega Remote on the hub. At initial startup, you are not required to enter a password. You may configure a system password later (described in Chapter 3, “Password” on page 36).

Selecting Menu Options

There are two ways to make menu selections:

- If the options are numbered, type the appropriate number and press the **Return** or the **Enter** key, or
- If the options are not numbered, type enough characters of the option to distinguish it from the other options and then press the **Return** or the **Enter** key.

 For example, if the options are:

 Alpha
 Beta
 GAmma
 GRemlin

 Choose an option by entering either **A**, **B**, **GA** or **GR**. You can also enter “**?**” to display a HELP screen. To guide you, the screen displays the characters you type in uppercase, such as GAmma and GRemlin.

NOTE

Omega is generally not case-sensitive. The download password, however, is case-sensitive (described later in Chapter 3).

Choosing an option often leads to another submenu. You can either choose an option from the new menu or return to the previous menu by pressing **Return**, **Esc**, or **CTL+C**.

A few menus (e.g., `Port Status` menu for modules with high port count) cannot fit on a single screen. In this case the management agent displays “`more...`” on the screen. The remaining text will be displayed when you enter **M**.

All menus and messages are multilingual—you can choose a preferred human language from the following:

- English
- French
- German
- Italian
- Spanish
- Japanese

You can change the active language by using the `Language` command under the `Administration` menu.

Configuring Hub Modules in a Chassis

If you have a chassis configuration, the main menu lists the installed and active TurboStack modules, enabling you to control any module from a terminal connected to the master (the module in the uppermost slot). The main menu looks like the following screen:

```
     Allied Telesyn International AT-TS24TR Stackable Hub: 4.0

Please select an option:

   Port status
   Hub Statistics
   Module statistics
   Individual port overview
   Security/Source Address Table
   Administration
   Quit

Or select a module:

> 1-
   2-
   3-
   4-
   5-
   6-
   7-Allied Telesyn AT-TS90TR Ethernet Switch

->
```

The example shows a 7-slot *Turbo*Stack chassis configuration with six hubs and one Ethernet switch in the bottom slot. All seven modules share a segmented backplane. If all the slots were filled with *Turbo*Stack hubs only, the software can report up to eight hub modules sharing a standard backplane.

For more details about various chassis configuration, refer to the *TurboStack 4-, 7-, and 8- Slot Chassis and Backplanes Installation Manual*.

You can assign names of up to 20 characters to:

- Each module
- Each port on each module
- The hub as a whole

You can enable or disable security features for *each port* or *each module*. For example, if you want to restrict access to a specific port or module, you can lock the MAC address table and manually enter only the MAC addresses allowed to use that port or module.

NOTE

The security option is not available at the hub level. If you want to keep the entire hub secure, you must enable the security feature on *every module* in the chassis.

Ending a Session

End an Omega session by selecting `Quit` from the main menu. This returns the management agent to an idle, listening state and breaks the communication link. If connected via a modem, the phone circuit will be "hung up"; if connected via the network, the virtual circuit will be disconnected.

NOTE

An Omega session automatically quits if there has been no keyboard entry after five minutes. This ensures availability for the next management session. You may change the five-minute timeout value through the `Administration/Omega Options` menu.

Managing Remote Hubs

After setting up the first hub, you can connect to other *Turbo*Stack management hubs in your network to set them up. Use the Omega menus to connect to those hubs.

NOTE

In a non-TCP/IP network, you cannot connect to a remote hub across network routers.

To manage another hub in the LAN:

1. Select `Administration` menu from the Omega main menu.
2. Select `Connect to a remote hub`.
3. Enter the remote hub's MAC address if this is the first time you are connecting to it.

 In future sessions and after you have configured an IP address or name, you may also connect to the hub by those parameters.

 The Omega main menu on the remote hub appears.
4. Proceed with hub management.

To manage a remote hub management across a WAN:

NOTE

This procedure works only in TCP/IP networks. The target hub must have an IP address.

1. Connect a modem to the remote hub's serial port.
2. Select `Administration` from the Omega main menu on your hub.
3. Select `Connect to a remote hub` and enter the target hub's IP address.

 The Omega main menu on the remote hub appears.
4. Proceed with hub management.

Using AT-View®

You can purchase an optional network management package called AT-View from Allied Telesyn. This Windows®- and UNIX®-based SNMP software application offers an easy-to-use and inexpensive graphical user interface (GUI). AT-View is ideal for simple and fast diagnostics, configuration, and the monitoring of network devices.

AT-View allows you to perform network monitoring and management tasks such as:

- Assign names to hubs, modules, and ports
- Identify enabled/disabled ports
- Change the enabled/disabled status of ports
- Configure polarity correction
- Set reconnect algorithms
- Enable/disable link test

AT-View can track 20 current network statistics, including total collisions and errors. It also offers a graphing capability that facilitates tracking of network performance trends.

Chapter 3

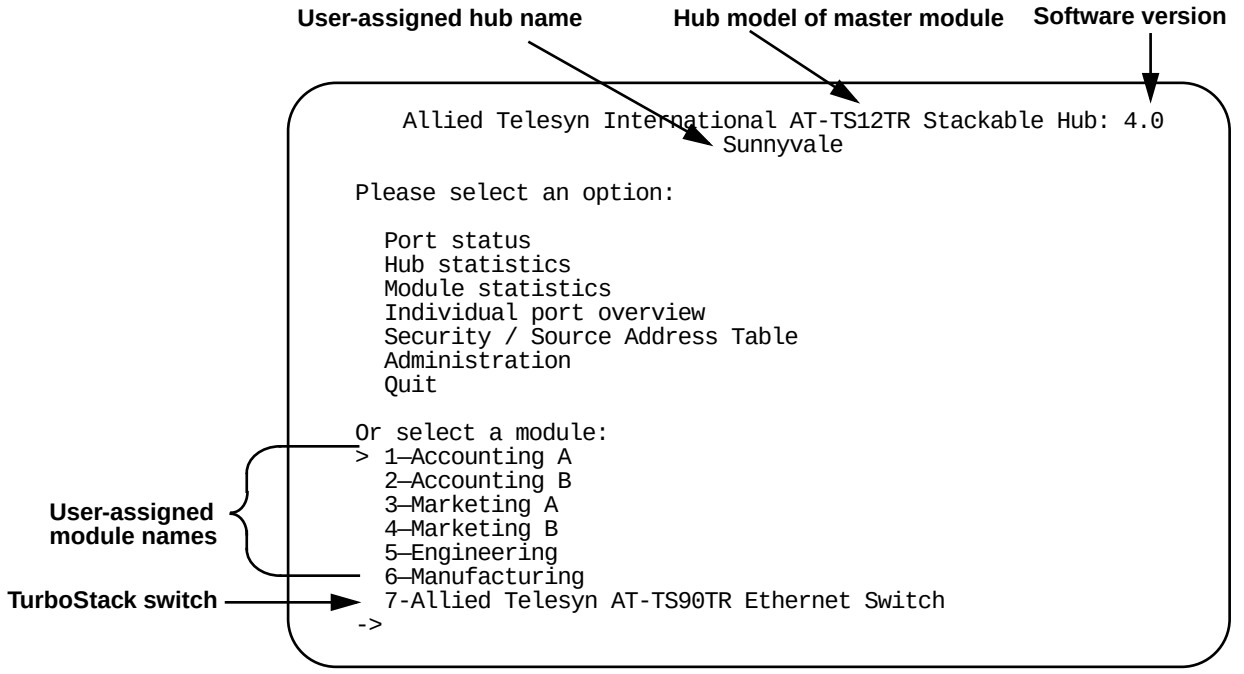
Management Menus

This chapter describes the Omega menus to configure and manage your *Turbo*Stack hub.

Main Menu

When a new session begins, the first screen you see is the main menu, as shown in the following example of a segmented backplane chassis configuration.

For illustration purposes, this chapter will show screens of a hub pre-configured with module names.



At the top of the main menu is the product name and software version, and immediately below is the user-assigned hub name, if any (**Sunnyvale** in this example). The hub modules occupy the first six slots of a seven-slot chassis, and have all been given names. A TurboStack Ethernet switch, the AT-TS90TR, occupies the seventh slot. At the bottom of the screen is a prompt (->), where the cursor is blinking, awaiting input.

The master module cannot manage the switch; that is, you cannot use the Omega menus to name the switch. The master, however, can detect and report the switch's identity and displays the model number on the screen.To manage the TurboStack switch, refer to your appropriate switch manual.

In the lower part of the sample screen, the available modules are displayed along with their respective names. The numbers correspond to the module's slot position within the chassis. The currently selected module is always highlighted with an arrow (>), **Accounting A** in the example. To select one of the modules, enter the module's slot position. For example, to select the **Manufacturing** module, enter **6**.

The master module retains configurations you enter for specific module numbers. If a new module replaces an old one in a given slot number, the new module inherits the configurations associated with that slot. For example, a new module installed in Slot 1 inherits the module name **Accounting A**, along with other information associated with the old **Accounting A**. The new **Accounting A** takes over the master functions.

In a standalone configuration (the hub is not installed in a department concentrator chassis), Omega has a simplified main menu:

```
     Allied Telesyn International AT-TS24TR Stackable Hub: 4.0
                              Sunnyvale

Please select an option:

  Port status
  Hub Statistics
  Individual port overview
  Security/Source Address Table
  Administration
  Quit

->
```

When following procedures in this manual to enter or select an option, you must first type a number or character corresponding to your choice and then press the **Return** or **Enter** key.

NOTE

Examples used throughout this chapter apply to 10Base-T *Turbo*Stack hubs. Screen displays may vary according to the type of appliqué port your hub is using. Check your appliqué manual for more details.

Port Status Menu

When you select `Port status` from the main menu, a menu similar to the following appears:

```
                              Sunnyvale
                        Module 1—Accounting A
                             Port Status

Port             MAC Address       Link      Status    MAC Learning

1: Room 1148  00A0D2 80016E     Online     Normal       Enabled
2: Room 1149  0000F4 C02789     Online     Normal       Enabled
3: Room 1150  0000F4 D0D070     Online     Normal       Enabled
4: Room 1151  00805F 84239F     Online     Normal       Enabled
5:            00805F 4810F2     Online     Normal       Enabled
6:            000094 4514A6     Online     Normal       Enabled
7:            00805F E49A0B     Online     Normal       Enabled
8:            080009 984673     Online     Normal       Enabled
9:            0000F4 D09603     Online     Normal       Enabled
10:           0000F4 C00520     Online     Normal       Enabled
11:           080020 681B97     Online     Normal       Enabled
12:           0080C7 68A081     Online     Enabled      Enabled
13:           --                --         Normal       Disabled

Enter a port number to change a port's configuration
- or hit Return to continue with no changes

->
```

AUI port →

This display shows the list of the selected module's ports, current status, and configuration. The display shows the MAC address last seen by the ports. The MAC addresses dynamically change every time the ports detect new addresses.

The last line represents the appliqué port configured as an attachment unit interface (AUI). In this example, it is being used as an uplink port; therefore, `Link` and `MAC Learning` are not applicable. After you have assigned a name to any port, the name appears after the port number, as in ports 1 through 4 above.

This display is automatically updated every few seconds when the management agent is configured for a terminal with cursor control capabilities (such as ANSI). When using terminals without cursor control, you can manually update the screen by pressing the space bar.

Port Configuration Menu

If you enter a port number, for example, **1**, from the `Port status` menu, the Port Configuration Menu for Port 1 of a 10Base-T hub appears:

```
                          Sunnyvale
                    Module 1 — Accounting A
                      Port 1 - Room 1148

Link State:             Online
Partitioning State:     Enabled
Polarity:               Normal
MAC Learning:           Enabled

Please select an option:

> Enable port - with automatic partitioning
  Disable port
> Standard IEEE reconnection algorithm
  Alternate reconnection algorithm
> Link test on
  Off — no link test
> Polarity correction
  No polarity correction

  Change port name
  Zero all statistics counters for this port
  View/Select redundant link
  Toggle port learning setting
```

This display shows the current status and configuration of the selected port. At the top of the screen you see the hub name, the selected module and its name, and the selected port and its name, if you have previously assigned one. Next are the port's status and configuration modes. At the bottom you see a list of menu options. Each currently configured choice is highlighted with an arrow (>).

Port Enable and Port Disable

Partitioning is the software's ability to disable a port if the port has detected an error in the network. This is to prevent the port from repeating the error.

Enable port with automatic partitioning. Entering **E** for this option means the hub software automatically changes the port's state to `Partitioned` once it detects an error. In this case, the user cannot change the ports' state back to normal. When the user fixes the error condition, the port status changes back to `Normal` based on a reconnection algorithm.

Disable port. Entering **D** for this option means you are manually turning the port off to prevent it from repeating traffic. You may want to manually partition a port for security reasons; for example, an office connected to that port is vacant and you want to prevent unauthorized connections. You can manually enable this port again by entering **E** at the prompt.

Reconnection

Standard IEEE reconnection algorithm. Entering **S** for this option specifies that a `Partitioned` port is automatically changed back to `Enabled` if this port **receives** or **transmits** data without collision for a period of 512 bit times.

Alternate reconnection algorithm. Entering **A** for this option specifies that a `Partitioned` port is automatically changed back to `Enabled` *only* if this port **receives** data without collision for a period of 512 bit times.

Link Test

Link Test On. Entering **L** for this option enables the module to perform a 10Base-T link pulse test on this port. If the link between this port and a device is good, the status screen shows the port to be `Online`. If the link is not good, for example, because the device is powered off or there is a break in the cable, the status shows this port to be `Offline`.

Link Test Off. Entering **O** for this option prevents the module from performing this test and link state for the port shows as blank (--). The port could still be online or offline, however.

Polarity

Polarity Correction. Entering **P** for this option enables the module to automatically reverse the port's polarity as appropriate. If the port's receive pair polarity is correct, the status shows as `Normal`. If the status shows as `Corrected`, that means the software has detected incorrect polarity and has automatically fixed it.

No Polarity Correction. Entering **N** for this option prevents the module from reversing polarity automatically; you must manually do so yourself. The port can still have normal polarity; however, if the status shows `Reversed`, that means the software has detected incorrect polarity but cannot correct it.

Change Port Name

This option allows you to specify a new name for the selected port.

1. Enter **C** for `Change port name` to display the following screen:

```
                        Sunnyvale
                  Module 1—Accounting A
                         Port 1

This port's current name is:
  Null (not currently configured)

Please enter a new name, or Return to retain the existing name:

  ->
```

2. Enter a new name of up to 20 characters for the port, or press **Return** to keep the current configuration.

 To delete an existing name, press **Spacebar** twice and press **Return**.

 The port list is updated with the port's new name, if you assigned one.

Zero Counters

This option clears all of the statistics counters for this port to zero.

Redundant Links Configuration

The redundant link feature allows you to configure an alternate path to a critical network resource; this resource can be the backbone or a server running critical applications. You can have up to 6 pairs on a 12-port hub and 12 pairs on a 24-port hub.

A redundant pair consists of a primary and a secondary port. After configuration, the primary port is enabled and the secondary port, disabled. When the primary port fails, the secondary port takes over until the primary port's error condition is resolved. See Figure 2 for topology samples.

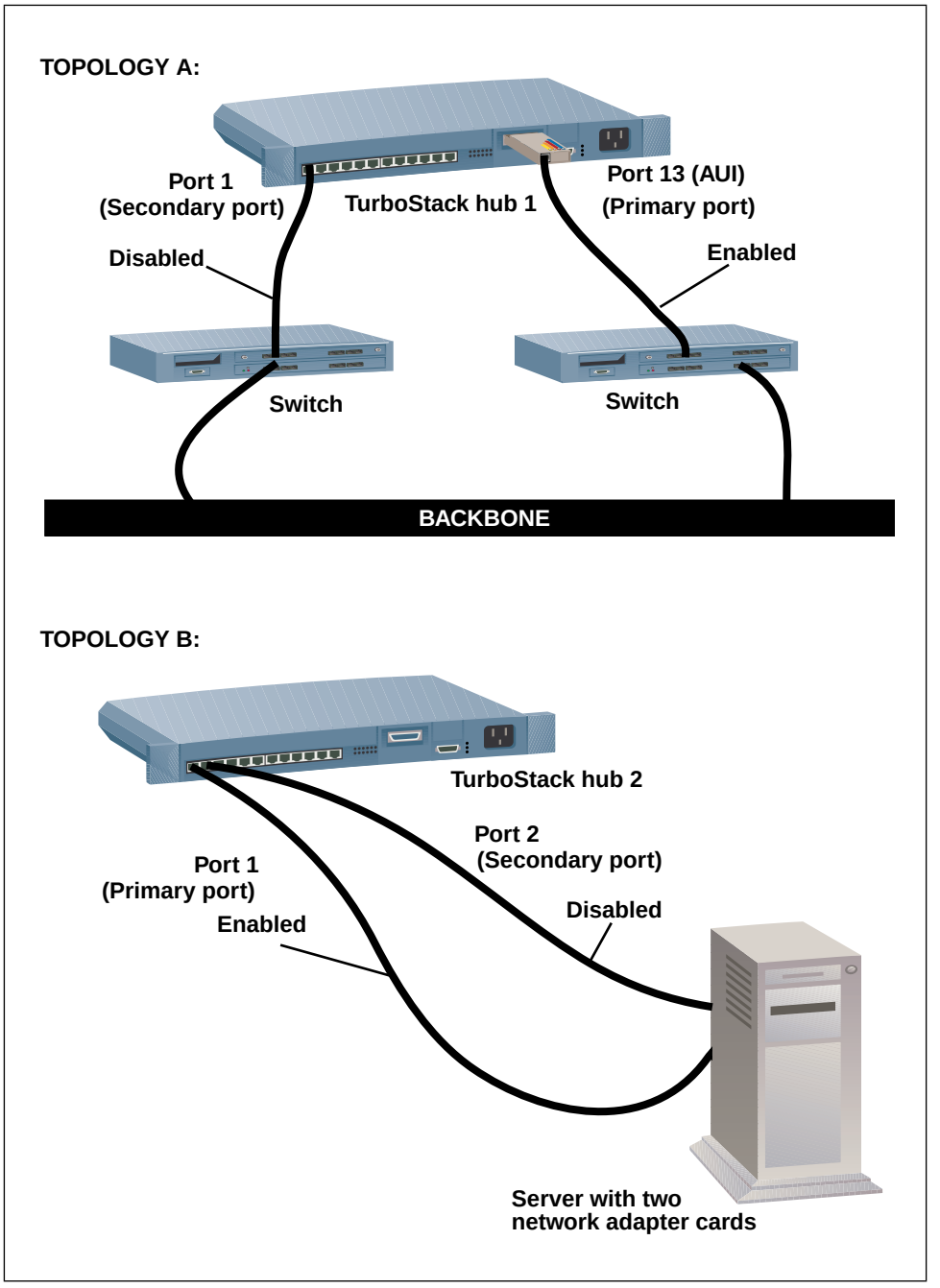


Figure 2: Redundant Link Topologies

Do not confuse redundant links with the spanning tree algorithm. Redundant links affect only the hub and its ports.

The software tests the primary port for the following failure conditions:

- **Loss of link -** If the primary port loses its link, the software automatically enables its secondary port. Once the link to the primary port is established again, the software automatically enables the primary port and disables its secondary port. The software defines the timing values to test the primary port (every 50 milliseconds), enable the secondary port if there is loss of link, and change back to the primary port (and also disable the secondary port) after the link problems are fixed.

NOTE

The software does not conduct link tests on AUI and 10Base2 (BNC) ports.

- **Autopartitioning -** The software automatically disables the primary port if there is an error, such as multiple collisions, or no data is received for a period of time specified by the `Receive Failure Timer`, and enables the secondary port. The software checks the primary port periodically (based on the `Check and Return to Primary Timer` value) and re-enables it if the error is corrected. The software rechecks by enabling the primary port (and disabling the secondary port) for a time period determined by the `Resample Timer`.
- **No data received -** The software automatically disables the primary port and enables the secondary port if no data is received for a period of time specified by the `Receive Failure Timer`. The software checks the primary port periodically (based on the `Check and Return to Primary Timer` value) and re-enables it if the error is corrected. The software rechecks by enabling the primary port (and disabling the secondary port) for a time period determined by the `Resample Timer`.

The software generates a private SNMP trap (defined in ATHUB.MIB) when a primary port fails and when it returns to normal.

CAUTION

Redundant pairs **must** belong to the same hub module. **Do not** cascade or duplicate redundant ports from one module to another; this configuration is not supported. If your redundant pair is a backbone connection, turn off learning on both ports (see "Port Learning" on page 25).

To define redundant ports:

1. Determine your port pairs, for example, Port 1 and Port 13 **of the same module**.

 In this procedure, Port 13 is your backbone connection and will become the primary port.

2. Select Port 13 from the `Port Status` screen.
3. Enter **V** at the `Port Configuration` menu to display the following screen:

```
                                Sunnyvale
                          Module 1—Accounting A
                                Port 13

                          Redundant Link Assignment

Secondary/(primary port)                  : Null (not currently configured)

Receive failure timer (secs)              : 60
Check & return to primary timer (secs)    : 60
Resample timer (ms)                       : 200

Please select an option:

  A: Secondary port

  Module settings:
  B: Receive failure timer (secs)
  C: Check & return to primary timer (secs)
  D: Resample timer (ms)
```

4. Enter **A** to display the next screen where you identify Port 13's secondary pair:

```
This port's secondary is: Null (not currently configured)

Please enter port number - or hit Return to continue with no changes

Please enter value, or zero to disable:
```

5. Enter **1** for Port 1; then press **Return** again to display Port 13's `Port Status` screen, partially shown below:

```
                              Sunnyvale
                        Module 1 — Accounting A
                      Port 13 - Primary port ->1

    Link State:Online
    Partitioning State:Enabled/RL
    Polarity:Normal
```

You have just defined one redundant pair. You may repeat the procedure to create more pairs. No more configuration changes are necessary; however, you may want to change the timer values.

To configure Receive failure timer:

The value you enter here has no effect if the primary port's failure is due to loss of link.

The timer indicates how long you want the software to wait before it enables the secondary port when the primary port is not receiving data. While waiting, there can be packet loss. To minimize this, you may want to enter a low value. The default is 60 seconds. If you do not want the software to check for received data, enter **0**.

1. Enter **B** to get the next screen.
2. Enter a value from 0-65,535 seconds.

When the secondary port takes over, the port status shows Port 13, the primary, as `Disabled/RL`; and Port 1, the secondary, as `Normal/RL`.

To configure `Check and return to primary timer`:

The value you enter here has no effect if the primary port's failure is due to loss of link.

When the primary port is autopartitioned or is not receiving data, the secondary port becomes enabled. Within the period you specify here, the software does not check the primary port.

The timer indicates how long you want the secondary port to remain enabled before checking if the primary port can receive data again or is no longer partitioned. The default is 60 seconds.

This parameter provides you the flexibility to adapt to your requirements. For example, you may base the checking time on how long it takes for someone to fix the problem once the SNMP trap is received. This may be **5** minutes on typical days. If you know how long a primary port cannot receive data because this port services an area in your building that is being remodeled for two days, you want this timer value to encompass or even exceed two days; but once this temporary condition goes away, you can reconfigure the timer back to your standard, routine value.

1. Enter **C** to get the next screen.
2. Enter a value from 0-65,535 seconds.

NOTE

If your `Check and return to primary timer` is **0** and the primary port fails, the secondary port takes over indefinitely. You must manually enable the primary port through the `Port status` menu.

To configure `Resample timer`:

The value you enter here has no effect if the primary port's failure is due to loss of link.

This timer indicates how long you want the software to test if the primary port is able to receive data or is no longer partitioned. This timer begins once the `Check and return to primary timer` has expired (five minutes based on the previous example). If the test shows that the primary port is still not receiving data or is still partitioned, the secondary port remains enabled. While sampling the primary port, the secondary port cannot transmit packets received. To minimize packet loss, you may want to enter a very low value. The default is 200 milliseconds.

1. Enter **D** to get the next screen.
2. Enter a value from 100-65,535 milliseconds.

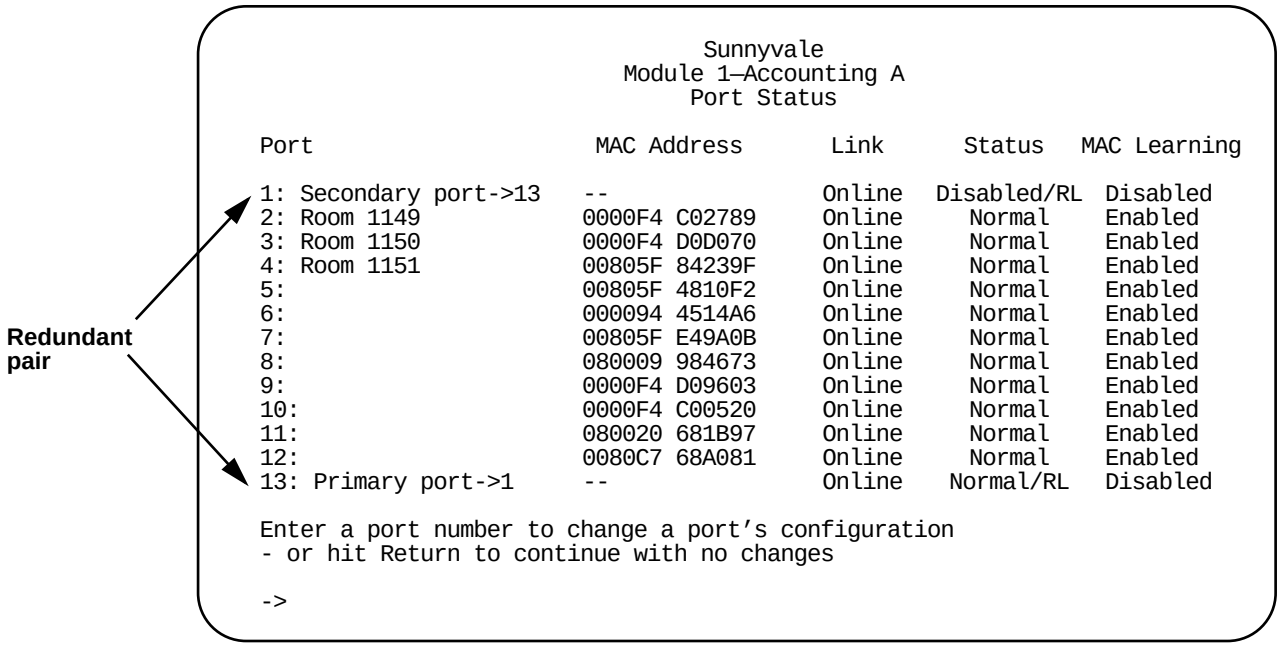
After entering the above values, you are taken back to the `Port Configuration` screen.

As primary port, Port 13 is enabled and actively receives and transmits packets. Port 1 is disabled until Port 13 fails. A secondary port's port configuration screen may be similar to the following example (partially shown):

```
                              Sunnyvale
                        Module 1 — Accounting A
                     Port 1 - Secondary port ->13

        Link State:Online
        Partitioning State:Disabled/RL
        Polarity:Normal
```

Press **Return** to go to the `Port Status` screen and to view the port list, which may be similar to the following example:



As you can see on the `Port Status` screen sample, redundant pair configuration writes over any previously-assigned port names. This enables you to see what ports you have paired together. If you want to change the name, it may be a good idea to use a name that also maintains their redundancy function (see "Change Port Name" on page 19 for the procedure).

NOTE

The software allows you to manually change the status of a redundant port. However, checks performed by the redundant link feature may immediately change the status again.

You are done with redundant pair configuration. You may proceed with the physical connections from your redundant ports to the network resource.

Port Learning

Selecting `Toggle port learning setting` changes a port's MAC address learning to `Disabled` if it was previously `Enabled`, and `Enabled` if it was previously `Disabled`.

All ports (except the AUI port) are in learning mode by default; they learn and store MAC addresses. If you want to use a port as a "network" port, that is, connected to the backbone, turn off its learning so it does not store uplink addresses. If your redundant link is a backbone connection, turn off learning on both redundant ports.

When you display the port list, the `MAC Learning` column shows the state of each port's ability to learn MAC addresses as the port detects new ones. `Enabled` means the port updates the MAC address table with any new MAC address it detects. `Disabled` means the port does not learn unknown MAC addresses on incoming packets.

AUI Port Configuration

The `Port status` menu for the AUI port is somewhat different, as some of the menu items do not apply to this port:

```
                          Sunnyvale
                  Module 1—Accounting A
                          Port 13

Partitioning State: Enabled

Please select an option:

> Enable—automatic partitioning control
  Disable—manual partitioning control

  Change port name
  Zero all statistics counters for this port
  View/Select redundant link
  Toggle port learning setting

  ->
```

Note that link integrity tests do not apply to this port.

Hub Statistics Menu

When you select `Hub Statistics` from the main menu, the following menu appears:

```
                              Sunnyvale

      Please select an option:

        Hub overview
        Module overview
        Individual port overview

        TOtal frames
        Good frames
        Bad frames
        Crc errors
        Alignment errors
        Runt frames
        LOng frames
        TRansmit collisions
        POrt collisions
        LAte collisions
        SHort events
        Jabber lockups
        PArtitions
        Data rate mismatches
        SOurce address changes
        Zero all statistics counters on the entire hub

      ->
```

The menu allows you to choose the level of statistical information you would like to see: from the hub to the type of Ethernet frame, also called counters. The counters, described in Table 1, are standard MIB objects.

Table 1: Types of Ethernet Frames

Frame Type	Description
Good Frames	Frames (packets) received without error.
CRC Errors	Frames with a Cyclic Redundancy Check (CRC) error, but with the proper length (64-1518 bytes) and no Collision or Alignment Error occurrences.
Alignment Errors	Frames with a non-integral number of bytes (i.e., the frame length in bits was not evenly divisible by 8), but with the proper length (64-1518 bytes).
Runts	Frames less than the Ethernet/IEEE 802.3 minimum frame length (64 bytes including the CRC).
Long Frames	Frames greater than the Ethernet/IEEE 802.3 maximum frame length (1518 bytes including the CRC).
Bad Frames	The sum of CRC Errors, Alignment Errors, and Long Frames.
Total Frames	The sum of Good Frames and Bad Frames.
Short Events	Frame fragments less than 74 bits in length.

Table 1: Types of Ethernet Frames (Continued)

Transmit Collisions	Frames with a collision occurring internal to the hub module; i.e., two or more ports attempted to transmit at the same time (available at the hub level only).
Jabber Lockups	Transmissions of excessive length that caused the hub module to enter Jabber Lockup mode (available at the hub level only).
Port Collisions	Frames with a collision occurring external to the hub module (an Ethernet collision signal detected); i.e., a port attempted to transmit at the same time as some other device external to the hub
Late Collisions	Port collisions that occurred after 64 byte-times of the frame had elapsed.
Port Partitions	The number of times the port was automatically partitioned Off Line.
Data Rate Mismatches	Frames transmitted at a data rate outside of Ethernet/IEEE 802.3 specifications.
Source Address Changes	The number of times a port or module detects a different incoming MAC address, even if the port or module has previously detected that address.

All of the Omega graph displays are automatically updated every few seconds when Omega is configured for a terminal with cursor control capabilities (such as ANSI). When using the terminal without cursor control, you can manually update the screen by pressing the spacebar.

Hub Overview

This option displays a summary of Ethernet frames the hub has processed since the last reset.

To view hub-wide statistics:

1. **S**elect `Hub overview` from the `Hub Statistics` menu to display a similar graph that combines statistical data from all modules:

```
                              Sunnyvale

  Good Frames:                 2163304 |######################
  CRC Errors:                   124456 |##
  Alignment Errors:              93342 |#
  Runt Frames:                   31114 |
  Long Frames:                       0 |
  Bad Frames:                   248912 |####
  Total Frames:                2412216 |######################
  Transmit Collisions:          108899 |#
  Port Collisions:                   0 |
  Late Collisions:                   0 |
  Short Events:                      0 |
  Jabber Lockups:                    0 |
  Port Partitions:                   0 |
  Data Rate Mismatches:              0 |
  Source Address Changes:            0 |
                                       ------------------------
```

Statistical information for the entire hub, specific modules, or all ports is displayed in the form of graphs. The graphs dynamically change as frames pass through.

2. Press **Return** to go to the `Hub Statistics` menu.

To display statistics per module:

1. Select a counter from the `Hub Statistics` menu.

 For example, enter **TO** to see the `Total Frames` graph, similar to the following:

```
                              Sunnyvale
                            Total Frames

Module 1—Accounting A:     2412216 |######################
Module 2—Accounting B:      123264 |###################
Module 3—Marketing A:       102720 |###################
Module 4—Marketing B:        87312 |############
Module 5—Engineering:       112992 |######################
Module 6-Manufacturing:      92448 |############
                                    ----------------------
```

 Module 7 is not included in the above example because it is a switch; therefore, the master module cannot report on its statistics.

NOTE

On a standalone hub, this graph is never displayed. If you select an Ethernet frame from `Hub Statistics`, a port-by-port graph is shown instead of a module-by-module graph.

2. Press **Return** to go to the `Hub Statistics` menu.

Individual Port Overview

This option requires you to enter a port number first, and then displays a summary of the selected port's activity. When you select the option from the `Hub Statistics` or the main menu, the port belongs to Module 1 by default, unless you first select a different module number from the main menu before `Individual Port Overview`.

Zero Counters

This option clears all of the statistics counters on the **entire module** to zero.

Module Statistics Menu

This option does not appear on a standalone hub.The default module is Module 1, unless you first select a different module number from the main menu. If you choose the `Module statistics` option from the main menu, the following screen appears:

```
                        Sunnyvale
                   Module 1-Accounting A

    Please select an option:

      Module overview
      Individual port overview

      TOtal frames
      Good frames
      Bad frames
      Crc errors
      Alignment errors
      Runt frames
      LOng frames
      POrt collisions
      LAte collisions
      SHort events
      Jabber lockups
      PArtitions
      Data rate mismatches
      SOurce address changes

      Zero all statistics counters on this module
    ->
```

Module Overview

This option displays a summary of Ethernet frames the module has processed since the last reset. This option offers several module-wide statistics functions.

To display module-wide statistics:

1. Enter **M** for `Module Overview` to display a similar screen:

```
                        Sunnyvale
                   Module 1-Accounting A

Good Frames:              2163304 |######################
CRC Errors:                124456 |##
Alignment Errors:           93342 |#
Runt Frames:                31114 |
Long Frames:                    0 |
Bad Frames:                248912 |####
Total Frames:             2412216 |######################
Port Collisions:                0 |
Late Collisions:                0 |
Short Events:                   0 |
Jabber Lockups:                 0 |
Port Partitions:                0 |
Data Rate Mismatches:           0 |
Source Address Changes:         0 |
                                  ------------------------
```

See Table 1 on page 26 for a description of the counters.

To display module statistics per counter:

1. Select a counter from the `Module Statistics` menu.

 For example, enter **T** to see the `Total Frames` graph, similar to the following:

```
                          Sunnyvale
                    Module 1—Accounting A
                         Total Frames

Port 1:Secondary port->13          0 |
Port 2:Room 1150                   0 |
Port 3:Room 1151                2031 |
Port 4:                            0 |
Port 5:                        33414 |###
Port 6:                        16707 |#
Port 7:                        66828 |#######
Port 8:                            0 |
Port 9:                        50121 |####
Port 10:                           0 |
Port 11:                       16707 |#
Port 12:                       33414 |###
Port 13:Primary port->1       116949 |############
                                     ------------------------

(hit Return to resume previous menu)
```

2. Press **Return** to go back to the `Module Statistics` menu.

Individual Port Overview

This option requires you to enter a port number first, and then displays a summary of the selected port's activity.

For example, Port 3's overview may be similar to the following:

```
                          Sunnyvale
                    Module 1-Accounting A
                            Port 3

Good Frames:              2163304 |######################
CRC Errors:                124456 |##
Alignment Errors:           93342 |#
Runt Frames:                31114 |
Long Frames:                    0 |
Bad Frames:                248912 |####
Total Frames:             2412216 |######################
Port Collisions:                0 |
Late Collisions:                0 |
Short Events:                   0 |
Jabber Lockups:                 0 |
Port Partitions:                0 |
Data Rate Mismatches:           0 |
Source Address Changes:         0 |
                                  ------------------------
```

Zero Counters

This option clears all of the statistics counters on the **entire module** to zero.

Security/Source Address Table Menu

Security options are enabled or disabled on a **per-module** basis only. The default module is Module 1. If you want to configure another module, for example, Module 5, select that module number first from the main menu before using the Security options.

When you select `Security/Source Address Table` from the main menu, a display similar to the following menu appears:

```
                                Sunnyvale
                          Module 5 - Engineering

Please select an option:
   A: display Source Address Table
   B: erase Source Address Table
   C: Add a MAC address to the table
   D: Delete a MAC address from the table

Source Address Learning Mode:
   E: Secure - source address table locked; intruder protection enabled
  >F: Learning - source address learning mode;intruder protection disabled

   G: Limit address per port to 1
  >H: Do not limit addresses
```

Source Address Table (SAT)

In this guide, source address table is interchangeable with MAC address table.

The following options are available:

- You can view and edit the table that lists the MAC addresses detected by ports.
- You can search for the MAC addresses detected by one port, or enter a MAC address and find out what port detected it.

When you enter **A** for `display Source Address Table`, the screen prompts you for the following choices:

```
                            Sunnyvale
                      Module 5 - Engineering

 Please select an option:

   Display MAC addresses for all ports

   Show MAC address for one port

   Find MAC address and display port

       (hit Return to resume the previous menu)
```

At the prompt, enter one of the following:

- **D** if you want to see the MAC addresses seen by all ports
- **S** if you want to see a single port
- **F** if you are searching for a specific MAC address

The following example is the SAT when you select **D**:

```
                        Sunnyvale
                   Module 5-Engineering
               Source Address Table - Page 1

MAC Address       Port        MAC Address       Port

00AA00 5E3DC2     11          0000F4 B1567E     21
00C07B 4D06D3     2           00AA00 5E3710     15
080009 95D13D     10          080020 74A55B     8
080009 2ADA9D     5           080009 9BDB2B     12
080009 2B7489     13          080009 681B97     18
080009 1DFEB5     1           080009 6F5610     4
080009 16BA5A     17          080009 984673     9
080020 739089     3           080020 715907     6
00000C 18E2F3     14          0000F4 E43068     7
00A0D2 000285     16          0000F4 D03D18     20

Please select an option:
  Next page
  (hit Return to resume the previous menu)
```

The SAT stores up to 300 MAC addresses per module in volatile memory and displays 20 addresses per page. The table also displays the ports where the addresses were detected. During the learning mode, the page number increases as the table is updated with more MAC addresses until the 300th address is detected (page 15 of the SAT). If any port has not detected a MAC address since the last power reset, the address entry for that port is blank (---). MAC addresses aren't fixed to the ports; the hub relearns a MAC address if you move a device to another port.

3. Press **Return** to go back to the previous menu.

To edit the Source Address Table:

You can edit the SAT whether the module is in secure or learning mode.

1. Select one of the following options from the `Security/Source Address Table` menu:
 - ❑ Enter **B** to erase the addresses in the table.

 When you erase the table while the module's learning mode is enabled, the system enters new addresses as soon as they appear on the ports. In case of a power failure while the learning mode is on, MAC addresses in the table are lost. However, once power is restored, the module quickly relearns addresses as long as the learning mode is still enabled for that module. In the secure mode, the SAT is saved and will survive power failures and module resets.
 - ❑ Enter **C** to add or **D** to delete a MAC address manually.

 When you manually add an address, the system does not enter a port number until it actually detects the address on one of the ports.
2. Press **Return** to leave the SAT screen and go back to the previous menu.

Learning Mode

The TurboStack hub has two modes of learning:

- Learning is on; security is off (the default)
- Security is on; learning is off

Regardless of the mode you select, SNMP statistics gathering continues.

NOTE

If you have a redundant links (RL) connection to a device with two network adapter cards (and therefore two MAC addresses), and your hub is in secure mode (and therefore learning is off), you must either allow the secondary port to learn the MAC addresses first; or enter the MAC addresses in the source address table.

Learning On. This is the default setting. In this mode, the SAT is in an "unlocked" state and is updated each time a port receives a packet from a new source address. The maximum number of addresses to store in the table is 300.

When the system is in a learning mode, the software:

- Monitors the MAC source address continuously on each port of the TurboStack hub module
- Compares incoming source addresses to entries on the table
- Updates the table by storing new addresses

Most users typically keep the learning mode on to continuously update the MAC address table. Information in the table is useful for inventory management purposes, based on MAC addresses of the devices connected to the module. As an option, you can manually turn learning off and automatically go to a secure mode if you want to restrict the module only to specific MAC addresses.

Security On. In the secure mode, the learning feature is disabled and the MAC address table is in a "locked" state. MAC addresses are written to non-volatile memory and survive power failures.

To enable security and prevent intrusions:

1. Enter **E** to turn the module into secure mode.

 The lower portion of the screen displays the following intruder protection options:

```
Source Address Learning Mode:
  >E: Secure - source address table locked;intruder protection enabled
   F: Learning - source address learning mode;intruder protection disabled

   G: Limit address per port to 1
  >H: Do not limit addresses

Intruder Protection:
   I: send an SNMP Trap if an intruder is detected
  >J: do not send an SNMP Trap if an intruder is detected
   K: disable the port if an intruder is detected
  >L: do not disable the port if an intruder is detected
```

In a secure mode, the system detects intrusions by comparing incoming source addresses to entries on the table. Transmissions from addresses not found in the table are considered intrusions.

NOTE

The master associates the MAC address table with a specific slot in the chassis. For example, if you lock the MAC address table of the module in Slot 2 and later replace that module with a new one, the new module in Slot 2 inherits the locked MAC address table.

2. Select the intruder options you want, as follows:
 - ❑ Enter **I** for the software to send an **SNMP trap message** to the SNMP manager.

 The traps go to the addresses you specify in `Network parameters` under the `Administration` menu. The message contains enough SNMP MIB information to help you identify the hub, module, and port where the intrusion took place. The message also contains the MAC address of the intruding device.
 - ❑ Enter **K** for the software to **automatically disable the port**.

 Note that once the software disables a port due to an intrusion, all source addresses cannot use that port. The port remains disabled until you manually enable it through the port configuration menu for the module.
 - ❑ Enter **I** and **K** for the software to do both.

 Once the software disables a port due to an intrusion, all source addresses cannot use that port. The SNMP manager also receives the trap.

The default setting where both `J` and `L` are selected means the software does nothing during intrusions. If you want to keep the default, the only security feature you are using is keeping the MAC address table locked.

Administration Menu

If you select Administration from the main menu, the following menu appears:

```
                                Sunnyvale

          Please select an option:

            Hub name
            Module name
            Omega options

            Network parameters
            Terminal configuration

            Language/langue/idioma/linguaggio/sprache

            Send updated software to another hub
            Update software in all hubs
            Reset hub config to manufacturing defaults

            Activity monitor
            EtherMeter

            Diagnostics

            Connect to a remote hub
          ->
```

NOTE

The Module name option does not appear in a standalone configuration.

Hub Name Menu

If you choose the Hub name option from the Administration menu, the following new menu appears:

```
                                Sunnyvale

The Hub's current name is:
  Sunnyvale

Please enter a new name, or Return to retain the existing name:

->
```

You may enter a new name for the hub, up to 20 characters in length, or press **Return** to keep the existing name. To delete an existing name, **Spacebar** twice and then press **Return**.

Module Name Menu

If you choose the Module name option from the Administration menu, a menu similar to the following appears:

```
                              Sunnyvale
                        Module 1 — Accounting A

The module's current name is:
  Accounting A

Please enter a new name, or Return to retain the existing name:

->
```

The module defaults to Module 1, unless you first selected a different module number from the main menu.

You may enter a new name for the currently selected module, up to 20 characters in length, or press **Return** to keep the existing symbolic name. To delete an existing name, press **Spacebar** twice and then press **Return**.

Omega Options

Selecting Omega Options from the Administration menu leads you through different screens where you can enter values for the following available options:

- Password
- Timeout value
- Enable or disable Omega Local
- Enable or disable Omega Remote

Password. The password protects access to the Omega management agent software. The default is no password.

If you choose to use password protection, you must enter password at the start of each subsequent Omega session. You may enter a password of up to 20 characters, or press **Return** to keep the current configuration. Your password displays on the screen as you type it, but displays as a series of asterisks (****) the next time you see this screen. To delete your current password, press **Spacebar** twice.

Press **Return** to get the Timeout screen.

To override the password, insert the AT-S10 software cassette.

Timeout. The timeout option automatically ends the session if there has been no activity for the length of time specified in minutes. The default is 5 minutes.

Enter the time in minutes. One minute is the shortest amount of time you can configure. If your timeout value is **0**, you must select **Q** from the main menu to quit at the end of every session; otherwise, other Omega Remote sessions to the hub will be blocked. The timeout period protects the management software from unauthorized use when left unattended for a specified length of time.

Press **Return** to get the Omega Local screen.

Omega Local. The default is Enabled for Omega Local. That means you can access the menus from a terminal or PC connected to the hub's RS-232 port.

If you want to disable this option for security reasons, press any key. That means Omega is not accessible via the local interface or the network. This takes effect after quitting the local session. To override, insert the AT-S10 software cassette.

ATTENTION

If you disable Omega Local, do not quit prematurely. Once you do, you can no longer access the menus without first inserting the AT-S10 software cassette.

Omega Remote. The default is Enabled for Omega Remote. That means you can access the Omega menus from a remote location.

If you want to disable this option for security reasons, press any key. That means you can no longer access Omega from a remote location. You can still use SNMP to manage the hub remotely. To change the setting again, use Omega Local.

Network Parameters Menu

The Network parameters menu is used to configure IP and SNMP information. These network parameters apply to all TurboStack modules in the chassis on a TCP/IP network. Users on non- TCP/IP networks need not configure any of these network parameters.

When you enter N from the Administration menu, the following menu appears:

```
                              Sunnyvale

 Please select an option:

   A:Ip address:               Null (not currently configured)
   B:Subnet mask:              Null (not currently configured)
   C:Gateway address:          Null (not currently configured)

   D:SNMP Manager address:     Null (not currently configured)
   E:SNMP Manager address:     Null (not currently configured)
   F:SNMP Manager address:     Null (not currently configured)
   G:SNMP Manager address:     Null (not currently configured)

   H:Get community string:     public
   I:Set community string:     private
   J:Trap community string:    public

   K:Download password:        ******

   L:Location:                 Null (not currently configured)
   M:Contact:                  Null (not currently configured)

 ->
```

NOTE

If you remove the master after configuring network parameters, the backup module automatically inherits the information.

When configuring network parameters for the hub, the software warns you if you enter a wrong address format. You must then press **Return** to go back to the `Network parameters` screen.

Hub IP Address. Enter **A** to display the `Hub IP address` screen as shown:

```
                                    Sunnyvale

The current Hub IP Address is:
  Null (not currently configured)

Please enter a new value, or Return to retain the existing one.
Enter a value in the form of a.b.c.d, where a, b, c, and d are each in
the range 0-255. For example: 128.9.3.1
```

Then enter the IP address for the hub.

CAUTION

All modules in the chassis inherit this address. This may result in duplicate IP addresses if you use one of the modules as a standalone hub in the future. Remember to change that hub's IP address when it becomes a standalone hub.

Subnet Mask . Enter **B** to display the `Subnet mask screen` as shown:

```
                                    Sunnyvale

The current Subnet Mask is:
  Null (not currently configured)

Please enter a new value, or Return to retain the existing one.
Enter a value in the form of a.b.c.d, where a, b, c, and d are each in
the range 0-255. For example: 255.255.255.0
```

Then enter the Subnet mask if any.

Gateway Address. Enter **C** to display the `Gateway address` screen as shown:

```
                                    Sunnyvale

The current Gateway Address is:
  Null (not currently configured)

Please enter a new value, or Return to retain the existing one.
Enter a value in the form of a.b.c.d., where a, b, c, and d are each in
the range 0-255. For example: 128.9.3.1
```

Then enter the address of the default gateway (router) to be used by the hub when transmitting packets to another network or subnetwork.

SNMP Manager Address . Enter **D**, **E**, **F**, or **G** to display the SNMP Manager address screen as shown:

```
                                    Sunnyvale

The current SNMP Manager Address is:
  Null (not currently configured)

Please enter a new value, or Return to retain the existing one.
Enter a value in the form of a.b.c.d., where a, b, c, and d are each in
the range 0-255. For example: 128.9.3.1

->
```

Then enter the IP address of the SNMP management station that is to receive SNMP trap messages. You can enter up to four different addresses. Each selection, **D**, **E**, **F**, or **G** is independent and you can select these options in any order. For example, entering an address from option G only is valid.

"Get" Community String. The default value is public. If you want to change it, enter **H** to display the screen as shown:

```
                                    Sunnyvale

The current 'Get' Community String is:
  public

Please enter a new string, or Return to retain the existing one:

->
```

Then enter up to ten characters for the SNMP Get function.

"Set" Community String. The default value is private. If you want to change it, enter I to display the screen as shown:

```
                                    Sunnyvale

The current 'Set' Community String is:
  public

Please enter a new string, or Return to retain the existing one:

->
```

Then enter up to ten characters for the SNMP Set function.

“Trap” Community String. The default value is public. To change it, enter **J** to display the screen as shown:

```
                                Sunnyvale

The current ‘Trap’ Community String is:
  public

Please enter a new string, or Return to retain the existing one:

->
```

Then enter up to ten characters for the SNMP Trap community string.

Download Password. The default password, **ATS10** (in uppercase), displays as a series of asterisks for protection. If you want to change it, enter **K** to display the following screen:

```
                                Sunnyvale

The current Download Password is:
  ******

Please enter a new string, or Return to retain the existing one:

->
```

Enter the password you want the download process to use in sending software to other *Turbo*Stack hubs. If you change the password, make sure you configure the same download password for all *Turbo*Stack hubs so they can receive downloaded software. That is, the hub downloading the software and the hub receiving the software must use the same password. See the section “Download Password” on page 40 and “TFTP” on page 58, Chapter 5 for more information on how the download password is used.

Location String. This parameter is optional. Enter **L** to display the following screen:

```
                                Sunnyvale

‘Location’ is a string that identifies the physical location of
this device, e.g. “Second floor computer room” or “Joe’s office”.

The current Location string is:
  Null (not currently configured)

Please enter a new string, or Return to retain the existing one:

->
```

This string is displayed by SNMP management stations.

Contact String. This parameter is optional. Enter **M** to display the following screen:

```
                                    Sunnyvale

'Contact' is a string that identifies the person primarily responsible for
this device (someone to contact in case of problems), e.g., "Joe Smith".

The current Contact string is:
  Null (not currently configured)

Please enter a new string, or Return to retain the existing one:

->
```

Enter the SNMP `Contact` string that identifies the name of the person within your organization primarily responsible for this hub. You can include a telephone number if you want. This string is displayed by SNMP management stations.

Terminal Configuration Menu

If you select `Terminal configuration` from the `Administration` menu, the following new menu appears:

```
                          Sunnyvale

        Please select an option:

          ANSI – VT100-compatible
        > Generic "dumb" terminal

        > 8 data bits
          7 data bits

        > 1 stop bit
          2 stop bits

        > No parity
          Odd parity
          Even parity

        > Full duplex (echo)
          Half duplex (no echo)

          Data rate ("baud" rate)...

        ->
```

You may select several options to specify the characteristics of your terminal and the serial interface. Default options are highlighted with an arrow (>).

Omega supports the control codes that adhere to the American Standard Code for Information Interchange (ASCII) character set, listed in Table 2.

Table 2: Required Terminal Control Characters

Control Code	What It Does
Carriage Return hex 0D	Moves the cursor to column 1 of the current file
Line Feed hex 0A	Moves the cursor down one line; if at the bottom of the screen, scrolls the screen up one line
Backspace hex 08	Moves the cursor back one character space

Omega can also take advantage of selected special control (escape) sequences that the terminal may use for screen control. Table 3 lists these special sequences.

Table 3: Optional Terminal Control Characters

Control Code	What It Does
Home Cursor	Moves the cursor to the top left hand position
Erase Screen	Erases the entire screen, or erases from the current position to end-of-screen
Erase EOL	Erases from the current position to the end of the current line

Any changes to the configured terminal characteristics, terminal type, and half/full duplex, take effect immediately. For example, changing from half duplex to full duplex causes the management agent to begin echoing your input immediately. The software saves all changes and retains them during a power failure.

Any changes to serial interface options (data bits, stop bits, parity, data rate) are saved but do not take effect until the next management agent session; i.e., you must select **Quit** from the main menu and then press **Return** to begin a new session. When you are connected to the management agent through a virtual circuit connection over the network, these serial interface options have no effect; however, they will affect any later session with a directly connected terminal.

ANSI or DEC VT-100 Terminal. The `ANSI` option auto configures the management agent for the characteristics of an ANSI-standard terminal (essentially the same as a DEC VT-100 or similar). If you want the control codes in Table 2 and Table 3, select this terminal configuration option.

Generic or "Dumb" Terminal. The `Generic` terminal option, the default, configures the management agent for the simplest possible terminal type. The control codes available to you are those in Table 2 only. In this configuration, the management agent makes very few assumptions about the terminal's capabilities and is compatible with almost all terminal types.

Data Rate. Omega supports the following data rates:

- 19200 bps
- 9600 bps
- 4800 bps
- 2400 bps
- 1200 bps
- 600 bps
- 300 bps
- 150 bps
- 75 bps
- Automatic baud rate detection (the default)

It is best to keep the default configuration, automatic baud rate detection, by pressing **Return** twice. The two **Return**s determine the terminal's actual data rate. If you want to select a specific baud rate from the available options, enter the first character or two of your selection at the prompt.

Language Menu

When you select the Language option from the main menu, a new menu displays the following choices:

```
                              Sunnyvale

Please select an option:

> English/anglais/ingles/inglese/englisch
  French/francais/frances/francese/franzoesisch
  Spanish/espanol/espagnol/spagnolo/spanisch
  Italian/italiano/italien/italiano/italienisch
  German/deutsch/allemand/aleman/tedesco
  Japanese/japonais/japones/japonese/japanisch

->
```

If you select a different language, for example, **S** for Spanish, the menu reappears using the new language:

```
                              Sunnyvale

 Por favor seleccione una opcion:

   INgles/english/anglais/inglese/englisch
   Frances/francais/french/francese/franzoesisch
 > Espanol/spanish/espagnol/spagnolo/spanisch
   ITaliano/italiano/italian/italien/italienisch
   Aleman/deutsch/german/allemand/tedesco
   Japones/japanese/japonais/japonese/japanisch
 ->
```

The main menu in Spanish then appears as follows:

```
  Centro Extensible AT-TS12TR de Allied Telesyn International: 4.0
                              Sunnyvale

Por favor seleccione una opcion:
  Estado de puerto
  Centro - estadistica
  Modulo - estadistica
  Generalidades de puerto
SEcurity/Source Address Table
  Administracion
  SAlida

->
```

The management agent "remembers" and retains the selected language through a power failure. The language option in the Japanese version of the management agent offers only English and Japanese (Kanji).

Update Selected Node

This option allows you to send software from one hub to another.

If you select `Send updated software to another hub` from the `Administration` menu, you are prompted to select an individual hub node to download with new software:

```
                                Sunnyvale

Please specify the hub to be downloaded:

The Hub to be downloaded may be identified by name ('hub name'),
  by IP address (128.2.3.4), or by Ethernet address (0000F4 123456).

->
```

Specify the node to be downloaded by entering *one* of the following information:

- The hub's IP address if the node has already been configured with one
- The target hub's name if one has been configured, or
- The hub's MAC address

Update All Nodes

Perform this download during times when the network is not busy. You may need to repeat the procedure because not all hubs may receive the download the first time.

If you select `Update software in all hubs` from the `Administration` menu, a message is broadcast to all other TurboStack hubs, informing them about the download if they are not already running the current software release (the software running on the hub from which you issued this command). Hubs running older versions of the software send back a request for the new version.

After this message is broadcast, the management agent switches to Activity Monitor mode to enable you to monitor download activity. The screen displays messages similar to the following example:

```
                          Activity Monitor
                (hit Return to resume the previous menu)

Download request received from Third Floor Hub
Sending...: 00000 - 99999
Load completed
```

The numbers 00000 and 99999 are the beginning and ending addresses, respectively, of the portion of memory currently being downloaded.

Reset to Defaults

This option allows you to clear all your configurations (port names, hub names, and so on) back to the default, that is, the configurations provided by Allied Telesyn. When you select Reset hub config to manufacturing defaults, the software requires you to confirm.

Activity Monitor

This option displays a variety of messages showing system activity as it occurs. You enter this mode by selecting either the Activity Monitor option from the Administration menu. Network events are displayed as they occur. To return to the Administration menu, press **Return**.

The values displayed are for illustration only: your screen may display the values appropriate for the system you are configuring.

Sample department concentrator reconfiguration messages appear as follows:

```
                                Sunnyvale

module1 Accounting A is now online.
module2 Accounting B has been removed!
module4 Marketing B has failed!
```

Sample port reconfiguration messages appear as follows:

```
                                Sunnyvale

 module5, port12: Port is now partitioned.
 module3, port8: Port is no longer partitioned.
 module3 (Marketing A), port10: Port is now offline.
 module3 (Marketing A), port2: Port is now On Line.
```

The port number is replaced with the value AUI when appropriate.

If the master detects the presence of a slave that is not running the same version of the software, it displays the following message:

```
                                Sunnyvale

 Updating software in module5
```

If an unrecognized type of TFTP request is received, the following message appears:

```
                                Sunnyvale

TFTP request received from node >: Implied request ignored
```

The symbol **>** denotes the IP address of the requesting node in dotted decimal notation.

EtherMeter

The `EtherMeter` option on the `Administration` menu modifies the function of the port indicators on the current hub module's front panel. The indicators ordinarily display network activity on an indicator-per-port basis. Activating the `EtherMeter` option employs the indicators on a per-hub or per-module basis. The indicators cooperatively show a cumulative display of network activity, much like a graphic equalizer displays the volume of sound at a certain frequency.

```
                                Sunnyvale
                          Module 1 - Accounting A

Please select an option:

> Default LED display (per-port activity)

  EtherMeter
```

Diagnostics

The `Administration` menu's `Diagnostics` option enables you to run a limited set of diagnostic tests on the currently selected module's functionality. When you select this option, the management agent performs diagnostic tests and displays the results similar to the following display:

```
                                Sunnyvale
                          Module 1—Accounting A

Allied Telesyn AT-TS24TR Stackable Hub 4.0
MAC Address 0000F4 78126D
AT-S10 Advanced TurboStack Hub Manager: 4.0
Firmware Cassette Installed
Running 8 hours, 42 minutes, 15 seconds

Diagnostic Results:
  Flash PROM              Good
  Address PROM            Good
  RAM                     Good
  Network Interface       Good
  Serial Interface        Good
  MPR Chip                Good

           (hit Return to return to previous menu)
```

The top of the screen shows the user-configured hub name and selected module name. Below that is the module's model number (AT-TS24TR in this example), the module's MAC address, and the module's firmware version. It also indicates if a firmware cassette is installed.

The Diagnostics screen is the only place on the user interface where the MAC address is displayed.

The results for each test will either indicate Good or Failed. Diagnostic tests may be run on any module within a department concentrator. If the currently selected module has a failure and can no longer communicate across the backplane bus, the message "Module does not respond" appears. Note that these diagnostics are limited since they must be executed while the system is running, that is, not offline.

If any tests indicate a failure, contact Allied Telesyn immediately. See Appendix C, "Where To Find Us," for information on how to contact the nearest location.

Connect to a Remote Hub

When you choose Connect to a remote hub from the Main Menu, you see the following menu:

```
                                Sunnyvale

Please specify the hub to connect to:
  The hub may be identified by name ('hub name'),
    by IP address (128.2.3.4), or by Ethernet address (0000F4 123456)
```

This option initiates an outbound (Telnet) session from a *Turbo*Stack hub to other *Turbo*Stack hubs in your network, whether or not you have loaded IP addresses. This option is useful when you are managing remote networks. With a modem attached to the RS-232 port of one of the hubs at the remote site, you can dial into the network and directly manage the remote hub attached to the modem. Using the Connect command, you may then also manage other Allied Telesyn intelligent devices on the remote network.

NOTE

If you are specifying the hub by its user-assigned name, be sure to enclose the name in single quotation marks (e.g., **'Sunnyvale'**).

When the connection is established, you see the Omega main menu from the remote hub. When you are done, disconnect the Telnet circuit by choosing Quit form the main menu.

Chapter 4
Fault Tolerance

This chapter describes the behavior of master and slave hubs in terms of module failure in a chassis configuration. It also provides procedures on how to swap failed modules in the chassis.

CAUTION

NEVER power off modules while they are in the chassis, because modules are not isolated from the backplane. When power cycling, ALWAYS slide the module out first, disconnect the power cord, reconnect the power cord, and then slide the module back in.

As mentioned in Chapter 1, you can stack multiple *Turbo*Stack hubs in the same chassis with backplane and manage them via the master module. In a standard configuration, up to eight hubs can all operate together as one logical concentrator; they share 10 Mbps bandwidth. In a chassis with segmented backplane configuration (7-slot with internal switch or 8-slot with external switch), hub modules are each allocated 10 Mbps of bandwidth.

The **master** is defined to be the module in the lowest numbered (physically the topmost) occupied slot position. Typically this is slot 1, but it could be slot 2 if slot 1 is vacant. The other modules in the same backplane are called **slaves**. The master manages the modules in the chassis. With Omega, you can also use the master to configure and manage the switch. SNMP, however, treats each module as a independent units.

The first slave in the hub watches over the master and can take over a failed master's functions if that first slave has management capabilities. This special module is called the **backup**. This module is defined as the one occupying the next higher numbered slot position after the master. Use only *Turbo*Stack hubs with management capabilities as both master and backup modules.

As described in Chapter 1, a *Turbo*Stack hub running firmware AT-S10 cannot manage AT-3600 hubs. Refer to the section on AT-S10 and AT-S4 interoperability for details.

Department Concentrator Reconfiguration

Each module in a department concentrator of multiple hubs knows its own slot position within the chassis, and which other slot positions are occupied. From this information, each module determines whether it should act in the capacity of a master, backup, or slave. This process is called **role determination**.

Role determination occurs as soon as you power up or reset the department concentrator. Each module then begins to operate in its appropriate capacity. In addition, all of the modules constantly check the configuration of the department concentrator. If anything changes, role determination is repeated to make sure each module is performing its appropriate function. If you remove or add any modules, the entire department concentrator readjusts itself to the new configuration as necessary. Configuration changes are detected and the new role determination performed in less than two seconds.

If you remove the master, role determination causes the backup to take over as the new master. The module below the old backup (now the new master) takes on the role of a new backup. This process repeats if the new master is itself removed. Similarly, removing a backup causes a new module (the next module below the master) to take over as backup.

If you add a new master, that is, if you insert a new module above the current master, role determination causes the current master to relinquish control to the new module and to take on the role of backup; the previous backup, if any, then becomes a slave. Similarly, inserting a new module in an empty slot between the master and the backup causes the new module to take over as the department concentrator's backup.

Note that the AT-TS12FS/XX, AT-TS24TS, and the AT-TS24TRS models are manufactured as slave modules and can never assume the master function.

Module Failures

The masters and backups frequently exchange “handshakes” in order to verify proper operation. If the backup does not receive a handshake from the master after about two seconds, the backup concludes that the master has failed and then takes over the master's functions.

This takeover process is not the same as the role determination process described previously. In the case of the master's failure (not removal), the backup can take over the master's functions, but the chassis does not allow another module to take over as a new backup. Therefore, only a single level of redundancy exists in cases where the master fails but is not removed from the chassis.

If you removed the failed master, role determination causes the entire department concentrator to reconfigure itself with new master and backup. A new module then becomes the backup to the new master (the previous backup).

A failure of the backup cannot be corrected without removing the module itself; i.e., no other module can act as a backup for the backup.

Configuration Data

The master records all management agent configuration information in nonvolatile memory. This includes:

- The preferred human language for display
- Terminal characteristics
- Port configurations (enabled/disabled, etc.)
- User-specified port, module and hub names
- MAC address table

The master also copies this information into the non-volatile memory of each installed hub module. These copies are maintained in order to sustain department concentrator reconfigurations. The management agent remembers configuration data in spite of power failures, module failures, and module swapouts, even of the master itself.

When a backup takes over on behalf of a failed or removed master, it already has a current copy of all necessary configuration data. When you swap out the master and install a new module, the new master will receive correct and current configuration data from the Backup (previous master). This avoids the need to re-specify all of the configuration preferences. The process all happens transparently within seconds of the swapout.

Precedence

If you install a module from another network as the new master in a concentrator, it may contain some old configuration data from its previous existence (it may have been installed in a different department concentrator chassis at one time). When it begins operating in its new location, the master does not know if its own configuration data is correct or not. The backup has some data, but its data may or may not be the correct data for this particular chassis.

This issue between the two modules is resolved by an examination of their respective elapsed time counters (each maintains a time-since-last-reboot). If the backup has been up and running longer than the master, the conclusion is that the master must have just been inserted and contains "old" data. The data from the backup is more current and is therefore copied into the new master. But if both modules have just booted (presumably because you just reset the entire department concentrator) then the clock alone cannot determine whose data is correct (both clocks would read the same). In this case, the master attempts to resolve this through a process called **voting**.

Voting

During the voting process, the master polls each installed module and examines the stored configuration data.

The master declares the configuration data that is stored on the greatest number of modules as the correct data, that is, the majority rules. For example, if data set **A** exists on modules 1, 3, and 4, and data set **B** exists on module 5, the management agent accepts data set **A** to be correct and adopts this set of configuration data for subsequent use.

However, a dilemma occurs when there are only two modules installed in the chassis. In this case, there is no way to determine which data set is correct. The system defaults to the master data set, which might not be correct—you may need to reconfigure when swapping a spare into the master position of a two-module department concentrator. Reconfiguration is not necessary if you follow the swapping procedure.

Swapping Modules to Retain Configuration Data

Configuration data is always retained if module swapping occurs with **power applied**, that is, as long as one module remains powered up throughout the hot swapping procedure. This will cause the use of the proper data set based upon clock comparison as described above.

If you must remove power for any reason, you perform the swap by either of the following methods (these steps are only necessary in a two-module department concentrator).

Method one:

1. Pull out the old master.
2. Place the old backup into the master slot position.
3. Install the spare module in the backup position.

 The data set of the old backup is used.

Method two:

1. Pull out the old master.
2. Place the spare module below the old Backup, making the old Backup the new master.

 The spare module becomes the new backup.

Limitations exist when massive chassis reconfigurations occur. If all modules boot at the same time, the voting process occurs. If many modules have been swapped all at once, incorrect data could be used. If, for example, several modules had previously been installed together in a different chassis, they would all vote the same way and their (incorrect) data might be used. You can avoid this by:

- ❑ Making configuration changes incrementally, or
- ❑ Keeping backplane power on so that the master never needs to ask for a vote

With a standalone hub, however, there is not much the software can do when this single unit is swapped with a spare because there is no backup. You must reconfigure in this case. Note that the software allows you to reset the hub configuration to manufacturing defaults.

Chapter 5
Software Upgrades

This chapter describes the procedures to upgrade hub software.

The Omega firmware, AT-S10, is pre-loaded in manageable *Turbo*Stack modules at the factory and is ready to use. There are various ways to install or upgrade your firmware:

- Install the AT-S10 firmware cassette in the firmware port.
- Use TFTP.
- Upgrade the software in one *Turbo*Stack hub using the firmware cassette, and then download to other *Turbo*Stack hubs on the network.
- Connect a newly-bought *Turbo*Stack hub that has the latest firmware version to the network and then download to other hubs on the network.

NOTE

All *Turbo*Stack hubs on your network should be running the same version of software. If you are installing a new standalone hub into a network that has older *Turbo*Stack modules with old software, update the other hubs to the latest version. When mixing *Turbo*Stack and AT-3600 hubs in a chassis, all modules must be running AT-S4 firmware, version 3.0 or greater.

Using the Firmware Cassette

You can order an AT-S10 cassette (see Figure 3) separately for backup.

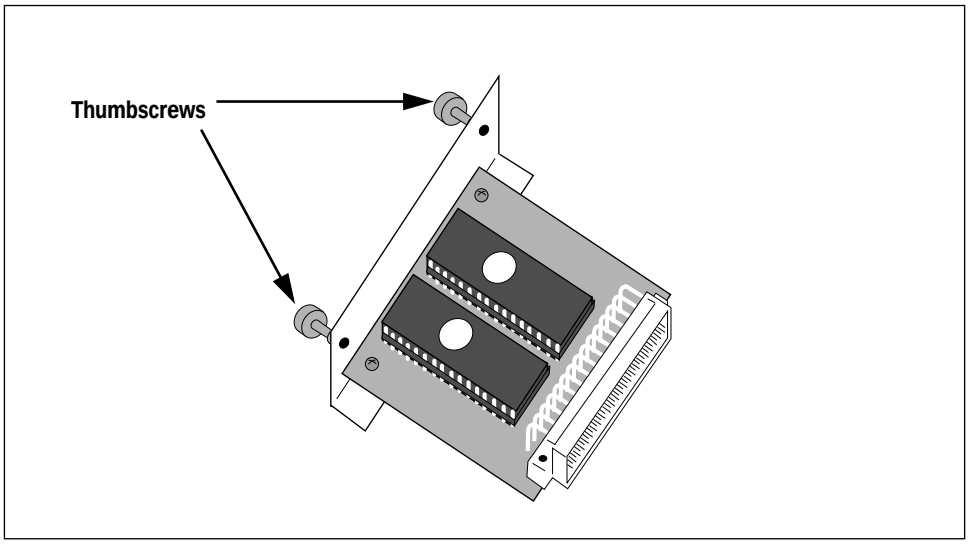


Figure 3: AT-S10 Firmware Cassette

You can use this compact cassette to override the login options for password protection and locking out Local Omega. The firmware cassette includes network management agent software for any manageable *Turbo*Stack module:

- SNMP Agent supporting MIB-II, and Repeater MIB (RFC 1516), and Allied Telesyn proprietary MIB (ATHUB.MIB)
- Unlimited site license
- Software downloading capability (receive and transmit)
- Multilingual Omega Telnet network management software agent

NOTE

When using the firmware cassette to upgrade management software on a network, first install the cassette into a standalone hub, upload the software, and then use this hub as master from which to download to all hubs and concentrators.

WARNING

Never power cycle hub modules while they are connected to the backplane. Disconnect them from the backplane first before removing their power cords to prevent damage to the backplane. Always plug in the hub's power cord before installing it in the chassis.

To reinstall or update the management agent using the cassette:

1. Remove the master from the chassis if this is a department concentrator configuration; otherwise, skip to Step 2.

NOTE

When removing any department concentrator module, always disengage the module from the chassis backplane before unplugging the power cord; i.e., use the hot swapping method. Refer to your chassis manual for more information.

The module is now a standalone hub.

2. Unplug the hub's power cord.

ATTENTION

Be sure to unplug the hub's power cord before installing and removing the firmware cassette.

3. Locate the blank cover plate on the firmware cassette slot on the hub's back panel (see Figure 4).

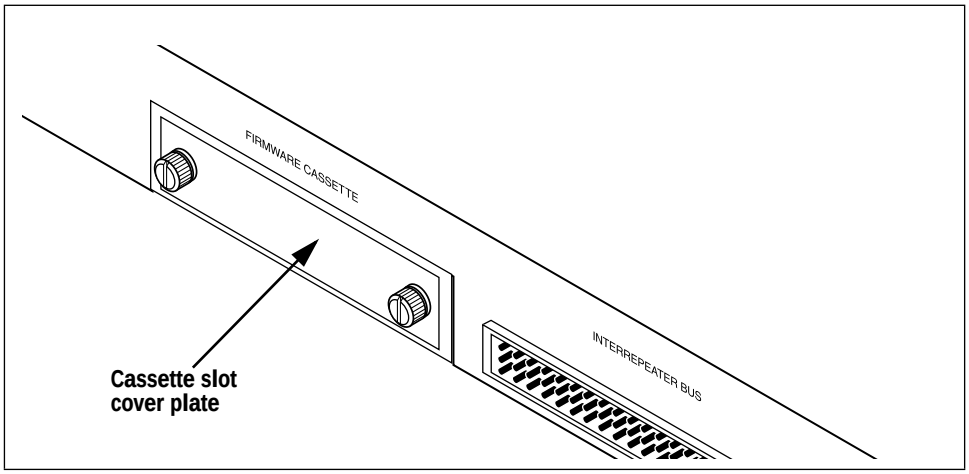


Figure 4: Cassette Slot Location on Hub's Back Panel

4. Turn the thumbscrews counterclockwise until they loosen, then grasp them to slide out the cover plate.
5. Slide the firmware cassette into the port, firmly pressing the connector into place; then turn the thumbscrews clockwise to secure the cassette to the hub's back panel.

 Make sure the firmware cassette is flush with the hub panel.

6. Plug the power cord into the hub.

 Downloading proceeds, taking up to two minutes. The hub's front panel LEDs flash continuously during downloading. The **FAULT** LED flashes once at the end of the download process.

7. Unplug the hub and remove the software cassette.

NOTE

You may leave the cassette installed. If you do, however, the module cannot receive downloads over the network. This is because the software network download does not overwrite a cassette. Password protection is also disabled when the cassette is installed.

8. Plug the power cord back into the hub.

 For a standalone hub, the software installation is complete.

9. Return the hub into the master uppermost slot in the chassis, if you have a department concentrator configuration.

 The other modules in the chassis are then automatically upgraded from the master with no impact to the users on those modules.

Using the Download Menus

The Omega software site license permits you to update other *Turbo*Stack hubs through the network. You don't need to insert an AT-S10 firmwrae cassette in each hub in the network or rack.

The download menus are for sending updated software from one *Turbo*Stack hub to other *Turbo*Stack hubs in the network.

Omega uses the trivial file transfer protocol (TFTP) of the TCP/IP protocol suite to download software to other switches whether or not your network uses TCP/IP. TFTP is transparent to other devices on the network. Make sure there is no firmware cassette installed in the hubs' firmware port, and they all have the same download password.

After updating the software in one hub, you can use the Omega menu on that hub to send updated software to specific *Turbo*Stack hubs, or to all.

NOTE

You do not need to issue download commands if you are upgrading modules via the master module. Once you insert a master module with the latest software into the uppermost slot of the chassis, it automatically downloads the software to other management hubs in the slots below.

To update a specific hub:

1. Select `Send updated software to another hub` from the `Administration` menu.

 The following screen appears:

```
                              Sunnyvale

Please specify the Hub to be downloaded:

The Hub to be downloaded may be identified by name ('hub name'), by
IP address (128.2.3.4), or by Ethernet address (0000F4 123456).

->
```

2. Enter either the hub's IP address, MAC address, or name.
3. The activity monitor appears, displaying messages about the download process.

To update all hubs:

Perform this procedure during those times when the network is not busy.

Select `Update software in all hubs` from the `Administration` menu.

The hub sends a broadcast message to all TurboStack hubs, informing them about the download, then turns on the activity monitor. All hubs running an older version of the software respond by requesting the updated software, and you see the messages on the monitor as each hub requests and then receives the updated software; for example:

```
                         Activity Monitor
              (hit Return to resume the previous menu)

Download request received from Third Floor Hub
Sending...: 00000 - 99999
Load completed
```

The numbers `00000` and `99999` are the beginning and ending addresses, respectively, of the portion of memory currently being downloaded.

TFTP

If you have a TCP/IP network, you can use TFTP to send or get the latest software. The source can be a *Turbo*Stack hub with the latest software or Allied Telesyn's Bulletin Board Services or web site. Check these services for the latest software (the image file) and the steps to download them.

Following are examples of TFTP commands.

To obtain a current image file, use the following command format:

tftp get <imagefilename><ip address> ATS10 octet

To download a current image file, use the following command format:

tftp put <imagefilename><ip address> ATS10 octet

You supply the IP address of either the file's source or destination. **ATS10** is the download password, and **octet** indicates that the file you are downloading is binary.

ATTENTION

The download password, **ATS10**, must be in uppercase.

Appendix A

Technical Support Fax Order

Name _____

Company _____

Address _____

City _____ **State/Province** _____ **Zip/PostalCode** _____

Country _____ **Phone** _____ **Fax** _____

Incident Summary

Model number of Allied Telesyn product I am using _____

Firmware release number of Allied Telesyn product _____

Other network software products I am using (e.g., network managers)

Brief summary of problem _____

Conditions (List the steps that led up to the problem.) _____

Detailed description (Use separate sheet, if necessary)

Please also fax printouts of relevant files such as batch files and configuration files. When completed, fax this sheet to the appropriate ATI office. Fax numbers can be found on page 63.

Appendix B

AT-S10 Management Software User's Guide Feedback

Please tell us what additional information you would like to see discussed in the manual. If there are topics you would like information on that were not covered in the manual, please photocopy this page, answer the questions and fax or mail this form back to Allied Telesyn. The mailing address and fax number are at the bottom of the page. Your comments are valuable when we plan future revisions of the manual.

On a scale of 1 to 10 (10 being most important), rate the importance of the following topics in this manual:

Overview _____
Getting started _____
Management menus _____
Fault tolerance _____
Software upgrades _____

I found the following the most valuable _____

I would like the following more developed _____

I would find the manual more useful if _____

Please fax or mail your feedback. Fax to 1-206-481-3790. Or mail to:
Allied Telesyn Technical Publications Department
19015 North Creek Parkway
Bothell, WA 98011 USA

Appendix C

Where To Find Us

For Technical Support or Service		
Location	Phone	Fax
Americas United States, Canada, Mexico, Central America, South America	1 (800) 428-4835	1 (206) 481-3790
Asia Singapore, Taiwan, Thailand, Malaysia, Indonesia, Korea, Philippines, China, India	(+65) 3815-613	(+65) 3833-830
Australia Australia, New Zealand	(612) 416-0619	(612) 416-9764
France France, Belgium, Luxembourg, The Netherlands, Middle East, Africa	(+33) 1-60-92-15-32	(+33) 1-69-28-37-49
Germany Germany, Switzerland, Austria, Eastern Europe	(+49) 30-435-900-126	(+49) 30-435-70-650
Hong Kong	(+852) 2-529-4111	(+852) 2 529-7661
Italy Italy, Spain, Portugal, Greece, Turkey, Israel	(+39) 2-416047	(+39) 2-419282
Japan	(+81) 3-3443-5640	(+81) 3-3443-2443
United Kingdom United Kingdom, Denmark, Norway, Sweden, Finland, Iceland	(+44) 1-235-442560	(+44) 1-235-442490
Technical Bulletin Board Service	1 (206) 483-7979	
CompuServe	Go ALLIED	
World Wide Web	http://www.alliedtelesyn.com	
FTP Server	Address: gateway.centre.com [lowercase letters] Login: anonymous [lowercase letters] Password: your e-mail address [requested by the server at login]	

For Information Regarding Allied Telesyn Corp.

Allied Telesyn Corp.
19015 North Creek Parkway
Bothell, WA 98011
Tel: 1 (206) 487-8880
Fax: 1 (206) 489-9191

Allied Telesyn Corp.
950 Kifer Road
Sunnyvale, CA 94086
Tel: 1 (800) 424-4284 (USA and Canada)
Fax: 1 (408) 736-0100

For Sales Information

Australia

Lindfield, NSW
Tel: (612) 416-0619, Fax: (612) 416-9764

Canada

Rexdale, Ontario
Tel: (416) 675-6738, Fax: (416) 675-0057

Richmond, British Columbia
Tel: (604) 244-0678, Fax: (604) 270-3644

England

Abingdon, Oxon
Tel: (+44) 1235-442500, Fax: (+44) 1235-442590

France

Les Ulis
Tel: (+33) 1-60921525, Fax: (+33) 169-28-37-49

Germany

Berlin
Tel: (+49) 30-435-90-00, Fax: (+49) 30-435-706-50

Freising
Tel: (+49) 8161-9906-0, Fax: (+49) 8161-9906-22

Hong Kong

Wanchai
Tel: (+852) 2-529-4111, Fax: (+852) 2-529-7661

Italy

Milano
Tel: (+39) 2-416047, Fax: (+39) 2-419282

Japan

Machida-shi, Tokyo
Tel: (+81) 427-21-8141, Fax: (+81) 427-21-8848

Yodogawa-ku, Osaka
Tel: (+81) 6-391-6310, Fax: (+81) 6-391-6325

Singapore
Tel: (+65) 383-3832, Fax: (+65) 383-3830

United States

Scottsdale, AZ
Tel: (602) 423-7087 Fax: (602) 423-7088

Los Angeles, CA
Tel: (310) 412-8684, Fax: (310) 412-8685

Mission Viejo, CA
Tel: (714) 699-0628, Fax: (714) 699-0276

San Diego, CA
Tel: (619) 279-3899, Fax: (619) 279-3897

Santa Ana, CA
Tel: (714) 838-0434, Fax: (714) 838-9721

Clearwater, FL
Tel: (813) 726-0022, Fax: (813) 726-0234

Norcross, GA
Tel: (770) 448-7214, Fax: (770) 448-2600

Reading, MA
Tel & Fax: (617) 944-3492

Eden Prairie, MN
Tel: (612) 829-7506, Fax: (612) 903-5284

St. Louis, MO
Tel: (314) 894-6160, Fax: (314) 894-3773

Dover, NH
Tel: (603) 743-3010, Fax: (603) 743-6327

Plaistow, NH
Tel: (603) 382-0815, Fax: (603) 382-0818

Portsmouth, NH
Tel: (603) 431-6461, Fax: (603) 431-1649

Morrisville, NC
Tel: (919) 468-0831, Fax: (919) 468-0829

Lake Oswego, OR
Tel: (503) 699-3130, Fax: (503) 636-6575

Austin, TX
Tel: (512) 261-6378, Fax: (512) 261-6379

Dallas, TX
Tel: (214) 365-9471, Fax: (214) 365-9472

San Antonio, TX
Tel: (210) 646-8744

Vienna, VA
Tel: (703) 506-0196, Fax: (703) 506-1986

Appendix D
Index

A
activity monitor, 45–46
alignment errors, 26
ANSI terminal type, configuring, 42
AT-S10
 cassette, 54
 installation, 44–45, 55, 56
 licensing information, 54, 56
AT-View, description of, 13
AUI port status, 17, 25

B
backup module, 2, 49
bad frames, 26
baud rates, terminal configuration, 43

C
cassette, firmware, description of, 54
chassis
 department concentrator, viii
 precedence, 51
 role determination, 50
 segmented backplane configuration, 49
 swapping modules, 52
 voting, 52
clearing statistical counters, 19, 30
community strings, 39–41
contact community string, 41
control characters, tables, 42
counters, 26–27
CRC errors, 26

D
data rate mismatches, 27
data rate *see* baud rates
DEC VT-100 terminal, configuring for, 42
defaults, resetting to, 45
department concentrator, *see also* chassis
diagnostics, 46–47

E
enable partitioning, port configuration, 18
EtherMeter, 46

F
failures, module, 50
forms
 fax, technical support, 59
 feedback on user's guide, 61
front panel, TurboStack hub, sample, 1, 20

G
gateway address, 38
generic terminal type, configuring, 42
get community string, 39
good frames, 26

H
handshakes, modules in chassis, 50
hub
 assigning names, 7, 35
 description of, viii, 2
 IP address, network parameter, 38
 modem, using with, 47
 remote, connecting to, Telnet, 47
 statistics, 27–28

I
intruder protection, 33–34
IP address, 38

J
jabber lockups, 27

L
languages, configuring for, 43
late collisions, 27
learning
 hub, 33
 port, 25
link test, 19
location community string, 40
long frames, 26

M
MAC address table, *see* source address table (SAT)
MAC address, where to find, 47
main menu, sample of, 6
management
 administration tasks, 35–47
 backup module, 2
 master module, 2
 network, 3
management information base (MIB), 54
manager address, SNMP, 39
manufacturing defaults, 45
menus
 activity monitor, 45–46
 administration, 35–47
 hub name, 35
 hub overview, 27–28
 hub statistics, 26–27
 language, 43–44
 main menu, sample of, 15–16, 44
 module name, 36
 module statistics, 29
 network parameters, 37
 port status, 17–25
 security, 31–34
 source address table (SAT), 31–34
 terminal configuration, 41
modem, using with hub, 47
modules
 assigning names, 36
 backup, 2, 49, 51
 configuration data, 51–52
 failures of, 50
 master, 2, 49
 precedence, 51
 role determination, 50
 slave, 2, 49
 swapping, 52
 voting, 52

N
naming hubs and modules, 35–36
network management, 3
network parameters, configuring, 37–41

P
password, entering, 36
planning, TurboStack installations, 3
ports
 collisions, 27
 configuration, 18–25
 learning, 25
 naming, 19
 partitions, 27
 polarity, 19
 redundant links, 20–24
 statistics, 28, 30
 status, 17–25
precedence, 51

R
reconnection, port configuration, 19
redundant links, 20–24
role determination, 50
runts, 26

S
security, 31–34
segmented backplane configuration, 49
set community string, 39
short events, 26
Simple Network Management Protocol (SNMP)
 MIBs, 54
 parameter configuration, 37–41
slave module, 2, 49
software downloading to hubs, 44–45
source address table (SAT), 31–34
statistics
 hub, 27–28
 module, 29–30
 ports, 28, 30
subnet mask, 38
swapping modules in chassis, 52

T

technical support
fax form, 59
locations, 63
Telnet management, 47
terminal configuration
control characters, table, 42
data rate, 43
terminal types, 41–42
total frames, 26
transmit collisions, 27
trap community string, 40
trap message
intrusions, 34
recipient, 39

V

voting, 52